Insights, News & Events

# "CLOUD"-Y WITH A CHANCE OF TRADE SECRET THEFT: HOW YOUR COMPANY CAN PROTECT AGAINST CLOUD-BASED DATA PILFERING

Publication
Nov 29, 2021

Misappropriation of trade secrets and confidential information used to involve an employee walking out the door with a box of records they spent hours copying after hours. As technology has advanced, departing employees have begun to misappropriate more efficiently. This usually involves emailing documents to personal Gmail accounts or transferring reams of data onto external hard drives or other USB storage devices. Some employees have found even their smart phones are a helpful tool to remove or store pilfered trade secrets. But now that many organizations have begun using cloud-based storage and filesharing platforms – which can be less expensive and easier for employees to use – employers are having a harder time protecting their assets by preventing departing employees from walking off with the electronic equivalent of the "box of docs." What can your company do to prevent this modern form of thievery and what can you do should you uncover it?

### Quick Quiz

Before we dive into specifics, here's a quick quiz to help set the stage. Which scenario is easiest for an employer to catch a trade-secret thief red-handed?

- Scenario 1: Clara Clepto is convinced that her list of customer contacts and pricing she developed over the years is *her* work product, so she believes she ought to be able to take it. She inserts a flash drive into the USB port of her laptop while no one is looking and then transfers all the files she needs onto the portable device. Clara pops

## Related People

**Stephen J. Roppolo**
Partner

713.292.5601

## Service Focus

Employee Defection and Trade Secrets

Privacy and Cyber

the thumb drive into her purse and heads home with all the documents she believes she is entitled to.

- Scenario 2: Freddie Freeloader knows that his employer is wallowing in cash and thinks he's entitled to a "parting gift" as he readies to leave for a competitor. So late one night while logged onto CashCo's system on his work-issued laptop, he uses his browser to access his web-based personal email account and attaches dozens of files from his laptop hard drive to emails he sends to himself and his girlfriend.

- Scenario 3: Louie Larceny accesses sales data for his most important customers right before leaving his employer and uploads it to his DropBox account using his Google Chrome browser. The electronic documents are still on his hard drive, so Louie is convinced that no one will have any idea that he uploaded copies to his personal Cloud-based account.

**To Catch A Thief: Ensuring Your Protection**

The good news for each thief's employer is that a proper computer forensic analysis of the employee's company-issued computer should detect each misappropriation scheme.

***Thumb Drives: Clara Clepto's Computer Caper Can Be Cut Off***

A USB history report can detect Clara's use of an external hard drive or flash drive by analyzing which devices are inserted into the laptop's USB ports. More importantly, the report can also indicate when the device is inserted and often can identify the device by serial number which makes it possible to demand the specific device once the analysis has been completed. Additionally, when used with a Windows registry report, a computer analyst can determine which files were accessed or transferred while the USB storage device was inserted into the laptop's USB port.

***Email: Freddie Freeloader's Fraud Can Be Frozen***

In addition, a simple review of an employee's email traffic in the weeks before their departure can uncover sloppy efforts to forward company materials to a personal email account. Like Freddie, most departing employees know not to use company email accounts to transmit proprietary documents

since it is so easy to trace. But even where he used a web-based personal email account through a browser on his work laptop, a forensic analysis should still be able to identify this form of misappropriation through a web history report.

***Cloud: Louie Larceny's Lawlessness Can Be Lulled***

Lastly, the same forensic analysis can detect access to a cloud-based storage account through the web history report (in combination with other forensic reports showing file access around the same time). So even the use of cloud accounts can be detested if you are willing to retain a forensic examiner to investigate whether the employee improperly accessed and transmitted company material.

**Cloud-Based Strategies for Deterring Digital Theft**

One difficulty in detecting the use of cloud accounts is when the employee returns their work-issued laptop in a "re-formatted" or "wiped" state. This should be a red flag for any employer in this situation, especially if the departing employee has even a rudimentary understanding of computers and the information that they can reveal about inappropriate activity. A re-formatted computer can prevent a computer forensic analyst from conducting the kind of investigation necessary to determine whether the employee left with a stash of company information.

This method of "covering your tracks" is essentially destruction of evidence, but it may not constitute legal "spoliation" (which can result in court-ordered sanctions) if the employee has no basis yet to believe that litigation is imminent. Therefore, it is a good idea to include in your IT or computer-use policy a prohibition against "re-formatting" or wiping a computer at any time during employment to minimize the risk that this might occur.

And even if it does, you can insist on inspecting the employee's flash drives and cloud-based accounts, especially if the employee is engaging in other activities that are suspicious. Sneaky contacts with key customers, odd network activity, and a computer "wipe" can be enough in many jurisdictions to warrant an examination of the departed employees accounts. This is especially true if the employee is also violating a valid restrictive covenant or is aggressively courting their old customers at a new employer.

Ultimately, the use of cloud accounts to stash misappropriated materials will not work if you can still conduct a forensic examination of a work-issued computer. But even where you work out an amicable resolution with a former employee to avoid misappropriation or restrictive covenant litigation, it is critical that you include any cloud storage accounts in the remediation process. It's great to have documents "zapped" from an employee's personal email account or to see a flash drive or personal computer searched to remove any misappropriated material, but employers sometimes forget to demand access to cloud accounts as part of this remediation process.

We will monitor developments in this area and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox. If you have further questions, contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our Employee Defection and Trade Secrets Practice Group.