Pirates and Rogues: Employee Theft of Trade Secrets and Proprietary Information

"or"

Jack Sparrow, Esquire's Tips for Battling Digital Raiders[1]

Mark Fijman

Phelps Dunbar, LLP

I. Introduction

> Me? I'm dishonest. And a dishonest man you can always trust to be dishonest. Honestly, it's the honest ones you want to watch out for, because you can never predict when they're going to do something incredibly ... stupid.
>
> ~ Captain Jack Sparrow

In the mid-18th Century, an owner of a merchant vessel on the high seas would clearly know when his ship came under pirate attack. Cannons would be fired and buccaneers armed with cutlasses would board the vessel, looking to carry off the ship owner's gold and other treasure.

In the modern workplace, the theft of an employer's treasure, *i.e.* trade secrets, proprietary information, customer data, is much less obvious but just as devastating. Unlike the pirates roaming the sea in the late 1700's, this theft is most likely to be carried out by a trusted and supposedly honest employee, usually for the benefit of a business competitor or to assist the employee in setting up his own competing business.

---

[1]All references to the character Jack Sparrow as an attorney are entirely intended as parody for educational purposes and as fair use under the United States Copyright Act and the Lanham Act. No affiliation is claimed with Walt Disney Studios and/or Jerry Bruckheimer Films. Likewise, no offense is intended toward any other actual or fictional 18th Century pirates by suggesting they may have attended law school, been admitted to any state bar association or engaged in the practice of law.

To paraphrase the observation above by the infamous Captain Jack Sparrow from the Pirates of the Caribbean movies, employers need to watch out for the employees they "think" are honest but who are actually getting ready to do something "incredibly stupid" and most likely, illegal.

This is further complicated by the now common "bring your own device" or "BYOD" practice of many employers, who allow employees to use their personal computers and smart phones to perform their workplace duties. When the employee eventually sails out the door to another job, the employer's trade secrets likewise can sail away inside the employee's iPad, iPhone or other device.

According to a 2013 survey conducted by computer security software company Symantec, more than half of departing employees kept confidential information belonging to their former employer and 40 percent planned to use such misappropriated trade secrets in their new jobs.[2]

The purpose of this article is to make employers aware of how such workplace theft can occur, how to best protect and defend your business against any would-be pirates in the workplace and the options for launching a legal counter-attack.

II. The "Pirate" Attack

> Worry about your own fortunes gentlemen. The deepest circle of hell is reserved for betrayers and mutineers.
>
> ~ Captain Jack Sparrow

The theft of company trade secrets and other information by former employees or executives has become so common, it regularly makes the news. For example, computer chipmaker Advanced Micro Devices just recently sued four former employees, alleging they stole hundreds of thousands of documents before leaving to work for a competitor.[3] In August 2012, a former Intel Corporation employee was sentenced to three years in federal prison for stealing Intel's confidential design information prior to taking a job with another high tech company.[4]

According to a 2010 statistical analysis, the annual costs associated with the theft of trade secrets and intellectual property were estimated at that time to be as high as $300 billion dollars a

---

[2] Symantec and Ponemon Institute, *What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk*, SYMANTEC WHITE PAPER (2013) (http://www.symantec.com/products-solutions/families/advantages.jsp?fid=data-loss-prevention).

[3] Don Jeffrey, *Ex-AMD Workers at Nvidia Lose Bid to End Secrets Lawsuit*, BLOOMBERG.COM (June 10, 2013) (http://www.bloomberg.com/news/2013-06-10/ex-amd-workers-at-nvidia-lose-bid-to-end-secrets-lawsuit.html).

[4] Federal Bureau of Investigation Press Release, *Former Intel Employee Sentenced to Prison for Stealing Valuable Computer Chip Manufacturing and Design Documents*, FBI.GOV (Aug. 8, 2012) (http://www.bloomberg.com/news/2013-06-10/ex-amd-workers-at-nvidia-lose-bid-to-end-secrets-lawsuit.html).

year, and that number has only risen in the ensuing years.[5] However, such theft is not limited to large corporations, and businesses of any size can fall victim to such misappropriation.

In the most typical instance, an employer will not be aware its trade secrets or proprietary information have been stolen until it discovers the information is already being used to lure away its business and customers. The following hypothetical scenario illustrates the very real types of improper conduct now common in the American workplace.

> Port Royal Industries ("PRI") is a successful marine engineering company founded twenty-five years ago by its owner, Will Turner. Back when PRI was a small family business, Turner hired Hector Barbossa and Edward Teach for entry level positions. They ultimately became top executives and corporate officers. Turner considers them friends and trusted employees.
>
> Because of the level of trust Turner has in Barbossa, Teach and all of his employees, PRI has never required its employees to sign non-disclosure, non-solicitation or non-compete agreements. Because of the "family business" atmosphere, Turner is somewhat lax about security for the Company's computer network, where PRI's proprietary designs and customer information are stored. Barbossa has a company-owned laptop which he uses for work, while Teach uses his personal iPad to perform his duties.
>
> Late one Friday afternoon, Turner receives an e-mail from Barbossa, informing him that Barbossa, Teach and three of PRI's top design engineers are resigning, effective immediately.
>
> Turner learns that Barbossa, Teach and the engineers now work for PRI's chief competitor, Black Pearl Enterprises ("BPE"). After the return of Barbossa's company laptop, a preliminary computer forensic examination reveals that days prior to the resignations, Barbossa downloaded thousands of PRI's engineering and design blueprints off its server and copied them onto external hard drives and flash drives. Computer professionals examine PRI's server and determine that the day before he resigned, Teach used his iPad to remotely access and copy PRI's confidential customer and pricing information.
>
> The forensic examination also reveals that months prior to their resignations, Barbossa and Teach engaged in regular e-mail communications with the President of BPE. Among the topics discussed in the e-mails are their plans to leave PRI, how the abrupt loss of the three design engineers will cripple PRI's ability

[5] David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum & Jill Weader, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. R. 291 (2010)

to serve its customers, and PRI's internal pricing information for key customers.

BPE is now aggressively competing against PRI and has been able to underbid PRI on a number of projects using the stolen pricing information. Utilizing the misappropriated design information, which they otherwise would not have been able to obtain through legitimate means, Barbossa and Teach have been able to take a number of key customers away from PRI.

An angry Will Turner contacts the law firm of Davy, Jones & Locker, LLC, to determine the best way to give Barbossa and Teach a legal keelhauling, and makes an appointment to meet with the firm's top employment attorney, Jack Sparrow, Esquire.

Unlike his famous cousin of the same name, Mr. Sparrow has issues with sea sickness, and opted to attend law school as opposed to entering the family business of captaining sailing ships.

The tale of PRI, its mutinous former executives and the piracy of its confidential business information will serve as the backdrop for how employers can avoid finding themselves in the unfortunate position of Will Turner. The advice from Jack Sparrow, Esquire also will show employers how to turn the tide against would-be boardroom buccaneers.

III. Best Practices to Avoid Trade Secret Theft by Employees

Prepare the cannons, wake all sailors and prepare to repel boarders.

~ Captain Jack Sparrow

In their first meeting, attorney Jack Sparrow agrees with Will Turner that Barbossa and Teach are indeed "scurvy dogs, yellow-bellied bilge rats and generally dishonest rapscallions." However, he advises that PRI could have avoided many of the problems now facing it by having had in place some basic policies and practices. "Not only would these policies have prevented or at least discouraged your two former executives from trying to pillage your business, but it would have given us additional legal claims to bring against these scalawags." Will asked, "what do we need to incorporate into our HR policies and practices."

A. Confidentiality / Non-Compete / Non-Solicitation Agreements

Sparrow explained, "One of the easiest ways to prevent employees from stealing your company's confidential information is to simply have them contractually agree in advance not to do it." For most companies, employee confidentiality is vital to a company's competitiveness. An employee confidentiality agreement establishes that an employee will keep the employer's confidential, private, secret and proprietary information private and confidential and that such information will not be disclosed to the general public or to outside third parties, such as competitors. Typically, such agreements also can prevent an employee's unauthorized use of

such information. Employee confidentiality agreements ensure that a company's private information and valuable knowledge stays where it belongs, within the company.

Sparrow noted that another option would be for PRI to have all of its higher level employees enter into non-compete / non-solicitation agreements. "These type of agreements prevent former employees from competing against you or soliciting your customers for a period of time after they leave the company."

In most states, these type of "restrictive employment covenants" are generally not favored, but will be enforced by the courts if the terms of the agreement are reasonable under the particular circumstances. Generally, there are three requirements: (1) the employer has a valid interest to protect; (2) the geographic restriction is not overly broad; and (3) a reasonable time limit is given. The employer bears the burden of proving the reasonableness of the agreement. The reason these types of agreements are construed very narrowly is that most courts recognize that an employer is not entitled to protection against ordinary competition from a departing employee."[6]

"In your instance" Sparrow observed, "you could justify the first factor because Barbossa and Teach were high level executives with access to confidential business and customer information, as opposed to one of your employees working on the loading dock. Courts look closely at the geographic restrictions of such agreements, because it would be against public policy for the restriction to be so broad as to prevent an individual from earning a living in his or her chosen field. For example, a restriction on competing within the entire United States would be considered overly broad and unenforceable. However, a limitation on competition in specific markets where you currently do business would be more likely to be enforced. As far as time restrictions, most courts will find a period of one to two years to be reasonable and enforceable."

Sparrow also remarked that to be enforceable, these types of agreements must be supported by sufficient consideration. When Turner looked puzzled, Sparrow explained, "In non-lawyer talk, that means that the employee had to have received something of value in exchange for entering into the agreement." What constitutes sufficient consideration can vary depending on the specific circumstances. However, in many states, courts have held that continued employment alone can be sufficient consideration to uphold a contract.[7]

If Barbossa and Teach had been required to sign these types of restrictive covenants as a condition of their employment or continued employment with PRI, their actions would serve as the clear basis for a breach of contract claim. "However", Sparrow noted, "because they never signed an agreement, that is one legal claim unavailable to us." Turner sighed and noted, "I never expected I would need to have my employees contractually promise not to be dishonest" and he and Sparrow made arrangements for Davy, Jones & Locker, LLC to draft such agreements for PRI to use going forward.

---

[6] *Business Communications, Inc. v. Banks*, 91 So.3d 1, 22 -23 (Miss. App. 2011) (citing 54A AM.JUR.2d *Monopolies and Restraints of Trade* § 905 (2009).

[7] *See Raines v. Bottrell Ins. Agency, Inc.*, 992 So.2d 642, 645-646 (Miss. App. 2008).

B. "BYOD" or Bring Your Own Device Policies

The subject then turned to Teach's use of his iPad to access and copy PRI's confidential customer and pricing information. Sparrow asked "How long has PRI allowed its employees to use their personal computers and devices for work, and what kind of policies do you have in place to regulate how they are used?"

Turner replied, "Well, about two years ago, we started letting employees link their work e-mail to their personal smart phones. Over time, I let people use their personal laptops and tablets because they tended to be more efficient and productive with their own devices. It also saved the company money because it spared us the cost of buying a company-issued gadget. We instead pay a monthly stipend to the employees who use their own devices. We really don't have any formal policy on how they are used."

"You're not alone," Sparrow said. "In one recent survey, 92% of the companies reported that they had employees using their own personal devices for work. However only 44% of those organizations had 'bring your own device' or "BYOD' policies that regulated the use of personal devices in the workplace.[8] Even those employers who have BYOD policies are constantly having to scramble to ensure they are still relevant in light of the constantly changing technology."

Sparrow continued, "While there are a lot of good reasons for having an effective BYOD policy, one key benefit is to prevent the misappropriation of your company's confidential information. In a recent corporate survey, the most pressing concern was that sensitive information will be on a personal device that is lost, stolen, or in the possession of someone who leaves the company or other theft of data via uploading to a personal device."[9]

Turner requested that Davy, Jones & Locker, LLC draft a BYOD policy for PRI, and asked, "What should our policy include?" Sparrow said, "There is no 'one-size-fits-all" policy, because every business is different and has different security and technology issues. He then outlined the following:[10]

- **Require devices to be pre-approved.** Sparrow pointed out, "Different gadgets have their own pros and cons when it comes to security, and your company's particular security needs will dictate which ones employees should be allowed to use."[11]

- **Have mobile device management (MDM) software installed. "**The two non-negotiable elements to look for in an MDM system are the ability to enforce security policies and to wipe remotely the personal devices used by employees." Sparrow further explained, "Such software typically requires a strong password

---

[8] Sam Narisi, *Let Users' Personal Devices Help: 5 IT Consumerization Policy Keys*, IT MANAGER DAILY (Jan. 25, 2012) (http://www.itmanagerdaily.com/it-consumerization-policy-keys/).
[9] *Michael Finneran, BYOD Requires Mobile Device Management*, INFORMATION WEEK.COM (May 7, 2011) (http://www.informationweek.com/mobility/business/byod-requires-mobile-device-management/229402912).
[10] *See supra* note 8.
[11] *See supra* note 8.

that's entered every time the device is turned on; ensures on-device file encryption; disables the camera; and specifies which applications are allowed, banned, or mandatory. It may also allow for monitoring to limit or deny access to certain company information.[12] Data loss prevention (DLP) technologies also can automatically flag when sensitive files are touched or an unusual number of files accessed or copied."[13]

- **Have employees agree in writing to security provisions.** "You can save yourself a lot of grief if you address the issue with employees on the front end," Sparrow said. "For example, an employee must agree to have their device remotely wiped if (1) the device is lost, (2) the employee terminates his or her employment, (3) if IT detects a data or policy breach, including unauthorized access to confidential company information, or (4) if there is any virus, malware or similar threat to the security of the company's data and technology infrastructure."[14]

- **Have an acceptable business use policy.** The policy should define acceptable business use as activities that directly or indirectly support the business of the company. Devices may not be used for unauthorized storage or transmission of proprietary information belonging to the company or misappropriated from another company, to engage in outside business activities, to harass others, view pornography, etc.

- **Disciplinary policy.** "Employees need to know there will be consequences for lax computer security when using their own devices for work," said Sparrow. "The company should reserve the right to take appropriate disciplinary action, up to and including termination for noncompliance with the BYOD policy."[15]

- **Have a plan for departing employees.** "The company should have a written agreement, signed by the employee, stating that the company's IT department will be allowed to inspect and delete all confidential information from the device when the employee leaves the company."[16]

- **Institute specific prohibitions on copying and forwarding of confidential information.** Sparrow noted that a common thread in these types of cases is the downloading and copying of company information onto external hard drives/flash drives, or the forwarding of confidential information by e-mail to an employee's personal e-mail address.

---

[12] *See supra* note 8.
[13] Sharon Nelson, How Digital Forensics Aids in the Investigation of Employee Data Theft, Ridethelightning.SENSEIENT.COM (May 20, 2013) (http://ridethelightning.senseient.com/2013/05/how-digital-forensics-aids-in-the-investigation-of-employee-data-theft.html).
[14] *See supra* note 8.
[15] *See supra* note 8.
[16] *See supra* note 8.

- **Prepare a Departing Employee Checklist so nothing is ever forgotten.** "The list itself will vary by the individual employer," Sparrow noted, "but might include changing office lock codes, collecting keys, asking questions about any personal devices that may have company data, having the employees sign a statement acknowledging that all company data has or will be returned and another statement acknowledging that any post-departure access to the network would be a criminal act."[17]

- **Consider other employment related issues.** For example, a non-exempt employee's use of a personal smart phone to check and respond to business – related e-mails or voice-mails off-the-clock can potentially expose an employer to liability under the Fair Labor Standards Act for unpaid wages or overtime. A BYOD policy should address when an employee is allowed to use the personal device for business purposes.

Sparrow added that along with the BYOD policy, "You also should have your IT department be on the lookout for any unusual activity that would suggest unauthorized accessing and/or copying of company information."

IV. Assessing the Damage/Preparing a Case

> I leave you people alone for just a minute and look what happens. Everything's gone to pot.
>
> ~ Captain Jack Sparrow

When a company suspects a former employee has stolen confidential information, time is of the essence, both to prevent additional losses, and to acquire and preserve digital evidence of the employee's wrongdoing to build a case against them. Sparrow told Turner, "A company that sits idly by while its trade secrets are being used unlawfully invites significant commercial harm, and even potentially risks waiving its rights to an injunction to protect those secrets, or even from claiming them as secrets at all. An employer should be ready to immediately implement an action plan."[18] This should include the following:

- Sparrow said, "you need to immediately lock the digital door". "Terminate any remote access privileges or user credentials that the employee may have to company proprietary information, and make sure that all company-issued electronic devices (e.g. laptop, smart

---

[17] Sharon Nelson, How Digital Forensics Aids in the Investigation of Employee Data Theft, Ridethelightning.SENSEIENT.COM (May 20, 2013) (http://ridethelightning.senseient.com/2013/05/how-digital-forensics-aids-in-the-investigation-of-employee-data-theft.html).

[18] Sid *Venkatesan* and Elizabeth McBride, *Using Computer Forensics to Investigate IP Theft*, LAW TECHNOLOGY NEWS (May 16, 2013) (http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202600258625&Using_Computer_Forensics_to_Investigate_IP_Theft_&slreturn=20130609180154).

phone, tablet, USB and external drives, etc.) have been returned. These steps should have been done at the time of the employee's termination but are sometimes overlooked." [19]

- "Not all the information you need will be on a computer," Sparrow noted. "Interview the employee's manager and co-workers about what the employee was working on, had access to, and whether there was unusual activity during the employee's last days, and whether the employee was acting secretively or left the company on bad terms."[20]

- Pointing to the computer on Turner's desk, Sparrow said, "A common mistake is for employers to immediately re-assign a former employee's computer equipment to another employee without first having it examined by a qualified expert. It is best not to even turn on or 'power-up' any such returned equipment," he warned. "Collect and sequester any electronic media (e.g. smart phones, laptops, and removable hard drives) that the employee used, and store it in a safe location accessible to one or only a few people to ensure the devices are not tampered with and that a chain of custody is preserved."[21]

- "You've already taken one important step," Sparrow said with a smile. "Retain outside counsel experienced in trade secrets and hacking cases to oversee the investigation and analyze the intellectual property and other legal rights which are available."[22]

- Sparrow also strongly stressed that any employer victimized by computer theft needs to "Retain an experienced computer forensic consultant."[23]

Sparrow told Turner, "While it is tempting for a company to rely on its in-house IT personnel to look for evidence of computer piracy, I always advise retaining an outside computer forensic expert to do the job. They typically have the specialized training and software to analyze the data without altering the contents or operating parameters of the devices and drives in question. This preserves the evidence for any litigation. A common practice is for the forensic expert to create an exact forensic 'image' of the device's hard drive for purposes of analysis, leaving the original device unaltered."

"What are the computer forensic experts looking for?," Turner asked. "Using specialized techniques and software, they are looking for proof that files or other information have been copied off the device or otherwise misappropriated," Sparrow explained. "A registry analysis will identify every external device that was attached to the computer by the date the device was connected, the time the device was connected, and the name and serial number of the device that was connected. It won't tell you who was on the computer at the time or which files were copied, but it will provide some evidence that can be followed up in further discovery that can establish

[19] *See supra* note 18.
[20] *See supra* note 18.
[21] *See supra* note 18.
[22] *See supra* note 18.
[23] *See supra* note 18.

the theft."[24] For example, Sparrow said, "If an analysis shows that Barbossa's laptop was used to illegally copy your files, and the copying was done on a date when he was the only one with access to the device, that can be strong evidence to support our case." Sparrow laughed and remarked, "It still amazes me how people will put the most harmful evidence in e-mails and texts, thinking they can destroy the evidence just by hitting 'delete'. We should be able to get a better idea of what Mr. Barbossa and Teach were up to once we get a good look at their e-mails."

"In some cases, you have employees who are more sophisticated about their computer theft and this is where computer forensics really pays off," said Sparrow. "Rather than copying files off a laptop, they may simply copy the entire hard drive using software such as Norton Ghost©, which creates an exact duplicate image which can be transferred to another computer or storage device.[25] They may then try to cover their tracks by using software like EvidenceEliminator© or Evidence-Blaster©."[26]

"However, this 'cleverness' can come back to bite them, said Sparrow. "While they may succeed in overwriting deleted data, making the files unrecoverable, the fact that they installed and then uninstalled evidence wiping software a day or two before they quit will remain in the registry. This raises the interesting question of what type of evidence is more damning, the forensic recovery of deleted files showing proprietary information was on the employee's computer but deleted, or the presence of unauthorized evidence elimination software that could only be present for the purpose of spoiling the evidence." [27]

Sparrow also noted that computer forensic information is important in determining what business losses can be attributed to the employee theft. "In any lawsuit, you'll bear the burden of having to prove money damages because of Barbossa and Teach's wrongdoing."

V. Legal Action Against Former Employees and Others

> Send this pestilent, traitorous, cow-hearted, yeasty codpiece to the brig.
>
> ~ Captain Jack Sparrow

Turner banged his fist on the table and demanded, "Is there anything I can do right now to stop these rogues? I'm afraid that by the time we get to trial, they'll have already sunk my business using my own trade secrets against me."

Sparrow said, "The first thing we can do is to ask the court to grant some immediate injunctive relief. Injunctive relief is an equitable remedy granted when money damages would not be enough to compensate you for your losses if an injunction was not granted."

---

[24] Bruce A. Olson, *Helping an Attorney Prove an Employee Theft/Theft of Trade Secrets Case with Computer Forensic Evidence: Part 2*, ONLAW TRIAL TECHNOLOGIES (June, 2, 2010) (http://www.dfinews.com/articles/2010/06/helping-attorney-prove-employee-theft/theft-trade-secrets-case computer-forensic-evidence-part-2).
[25] *See supra* note 24.
[26] *See supra* note 24.
[27] *See supra* note 24.

"The type of injunctive relief we'll seek is a temporary restraining order or "TRO" against Barbossa, Teach and BPE to prevent them from disclosing or utilizing PRI's trade secrets. We'll later move the court to leave it in place until our lawsuit can be decided on the merits. To obtain a TRO, we'll have to convince the court of four things: (1) that we're likely to succeed on the merits of our claims, (2) that PRI is being irreparably harmed by the improper disclosure and use of its trade secrets, (3) that Barbossa, Teach and BPE will not suffer irreparable harm if the TRO is granted, and (4) that the public interest is served by issuing the injunction."

Turner thought about what Sparrow had explained and said "Well, if I'm going to have to convince the court I'll succeed on the merits of my claims, I guess I better know what kind of claims I can bring. I think we've clearly and painfully established that it was a mistake for me not to have Barbossa and Teach under a restrictive covenant, and that rules out a breach of contract claim," said Turner. What other options do I have?"

Sparrow chuckled and said, "There's more than one way to have these treacherous scoundrels walk the plank!"

A. **Uniform Trade Secrets Act**

"In your case, there is statutory protection against the theft of your trade secrets by your former executives," said Sparrow. "Most states have adopted the Uniform Trade Secrets Act. The purpose of the Act[28] ("UTSA") is to prevent a person or business from profiting from a trade secret developed by another, because it would allow them to acquire 'a free, competitive advantage.'[29] To establish a claim of trade secret misappropriation under UTSA, we would have to be able to show: (1) that a trade secret existed; (2) that the trade secret was acquired through a breach of a confidential relationship or discovered by improper means; and (3) that the use of the trade secret was without the plaintiff's authorization." [30]

"So can you tell me what is considered a trade secret under UTSA?," Turner asked. Sparrow explained that under the Act, "A trade secret' means information, including a formula, pattern, compilation, program, device, method, technique or process, that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means, by other persons who can obtain economic value from its disclosure or use, and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." [31]

"Skip the legal jargon," Turner demanded, "What the heck does that mean?" "In essence," Sparrow said, "It means that a trade secret is something that is valuable to your business because it is not generally known outside your business, you take reasonable efforts to keep it secret, and the only likely way your competitor could find out about it would be by

---

[28] *See e.g.* MISS. CODE ANN. § 75-26-1 *et seq.*
[29] *Omnitech Intern, Inc. v. Clorox Co.*, 11 F.3d 1316, 1325 (5th Cir. 1994).
[30] *See Union Nat'l Life Ins. v. Tillman*, 143 F. Supp.2d 638, 643 (N.D. Miss. 2000).
[31] MISS. CODE ANN. § 75-26-3(d).

stealing it or through other improper means. Sparrow noted, "It would seem that the engineering designs that were stolen would meet the definition under UTSA."

"Would the customer information they took also be considered a trade secret?" Turner asked. Sparrow nodded "Courts interpreting this section of the UTSA have consistently held that lists of current and prospective customers, the requirements of customers, and other proprietary business information can constitute a trade secret."[32]

Sparrow continued, "UTSA refers to the theft of trade secrets as misappropriation. That means the acquisition of a trade secret by someone who knows or has reason to know that it was acquired by improper means, such as theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy. It also includes the disclosure or use of a trade secret without consent by someone who used improper means to acquire knowledge of the trade secret. For example, if an ex-employee spilled the company secrets to a business rival, who starts using the trade secrets."

"UTSA also prohibits the use of trade secrets by a company which 'has reason to know' that the material constitutes a trade secret. This is known as constructive knowledge (versus actual knowledge). In other words, even if a company was unaware it possessed purloined trade secrets, it can still be prosecuted if it *should* have known."[33]

Sparrow added, "With what we know right now, it looks like we have a good claim of misappropriation of trade secrets against Barbossa and Teach. In addition, we also should be able to go after BPE, because they clearly had reason to know that the information they were using belonged to PRI and was acquired by improper means. Under the Act, we can seek injunctive relief against them all and also seek money damages for the business losses they've caused to PRI."

B. Computer Fraud and Abuse Act

"Because of the way Barbossa and Teach stole information from PRI's computer system, you also can assert a claim under federal law, said Sparrow. Sparrow continued, "The Computer Fraud and Abuse Act ("CFAA)" provides civil remedies for certain types of misuse of computers and computer files.[34] "This law was originally enacted to bring criminal charges against computer hackers, but the civil component of the statute allows employers to seek damages against former employees for misuse of a protected computer," Sparrow noted. "CFAA defines a 'protected computer' as a computer 'used in interstate or foreign commerce or

---

[32] *See ACI Chemicals, Inc. v. Metaplex, Inc.*, 615 So.2d 1192, 1195 (Miss. 1993) (holding that trade secrets may be a list of customers and "may relate to the sale of goods or to other operations in the business, such as a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialized customers, or a method of bookkeeping or other office management") (quoting *Cataphote Corp. v. Hudson*, 422 F.2d 1290, 1293-94 (5th Cir. 1970)); see also *Zoecon Indus. v. American Stockman Tag Co.*, 713 F.2d 1174, 1179 (5th Cir. 1983) (noting that customer information can constitute a trade secret because it gives its owner "an advantage over competitors who did not have the information").

[33] Rich Stim, *Mississippi Trade Secret Law*, NOLO LAW (2013) (http://www.nolo.com/legal-encyclopedia/mississippi-trade-secret-law.html).

[34] 18 U.S.C. § 1030, *et seq*.

communication'[35] so a protected computer, in effect, could include any computer connected to the Internet.[36]

CFAA prohibits numerous types of conduct, including the theft of data from a protected computer and the unauthorized access of a protected computer resulting in damage to a protected computer.[37] Sparrow pointed out to Turner "The crucial evidence to support a successful CFAA claim will be the information you obtain from the forensic examinations you conduct early in the litigation process"

C. **Breach of Fiduciary Duty**

"What really bothers me about all this is that these two mutinous swine were my top executives and officers in the company and they were actively conspiring with my competitor. They were supposed to be working on behalf of PRI," Turner said to Sparrow. "Surely that can't be legal! Is it legal?"

"No, it's not," said Sparrow. Because they were trusted high level executives and corporate officers, they owed a legal duty of care and loyalty to your company. Because they clearly and intentionally worked against the best interests of PRI, we have a strong claim against them for breach of fiduciary duty!"

Sparrow explained to Turner that under the law in most states, a corporate officer has a duty of care which can be defined as follows:

> A director or officer has a duty to the corporation to perform the director's or officer's functions in good faith, in a manner that he or she reasonably believes to be in the best interests of the corporation, and with the care that an ordinarily prudent person would reasonably be expected to exercise in a like position and under similar circumstances.[38]

Sparrow continued, "The second fiduciary duty that all officers owe to their employer is that of loyalty, good faith and fair dealing. Officers have a duty to exercise 'the utmost good faith and loyalty' to the corporation.[39] This includes the duty to refrain from engaging in self-dealing activities."[40]

---

[35] 18 U.S.C. § 1030(e)(2)(b).
[36] *See United States v. Drew*, 259 F.R.D. 449, 458 (C.D. Cal. 2009).
[37] 18 U.S.C. § *1*030(a).
[38] *Omnibank of Mantee v. United Southern Bank*, 607 So.2d 76, 84 (Miss.1992).
[39] *Rogers v. The Mississippi Bar*, 731 So.2d 1158, 1168 (Miss. 1999) (citing *Ellzey v. Fyr-Pruf, Inc.*, 376 So.2d 1328, 1332 (*Miss.* 1979)); *see also Hill v. Southeastern Floor Covering Co.*, 596 So.2d 874 (Miss. 1992) (citing *Fought v. Morris*, 543 So.2d 167,171 (Miss. 1989)); *Gibson v. Manuel*, 534 So.2d 199, 201 (Miss. 1988).
[40] *Rogers*, 731 So.2d at 1168.

"In this case, Barbossa and Teach are clearly fiduciaries because of their high level positions within the company. However, courts have recognized that even lower level employees, such as a store manager or an office manager, also may owe such fiduciary duties to their employer, depending on the individual circumstances."

Looking through copies of the e-mails between Barbossa and Teach and the President of BPE, Sparrow said, "In these e-mails, your two back-stabbing executives are actively discussing with your chief competitor how to do damage to PRI. They're doing this while serving as company officers and top executives who are 'supposed' to be working in the best interests of your company. This is hardly the conduct of loyal employees acting in good faith. These e-mails are 'the smoking gun' in our breach of fiduciary duty claim against them! Plus, juries generally don't care for sneaky dishonest employees who are foolish enough to discuss all their wrongdoing in an e-mail."

Turner asked, "Is there any type of claim we can bring against BPE? What about the engineers who left with Barbossa and Teach? They had to have known what those two pieces of shark bait were up to, and helped them to steal our information!"

Sparrow nodded and said, "A person or a corporation 'who knowingly joins with or aids and abets a fiduciary in an enterprise constituting a breach of the fiduciary relationship becomes jointly and severally liable with the fiduciary for any profits that may accrue.' In other words, if BPE, its President or your former engineers knowingly helped Barbossa and Teach in breaching their fiduciary duties to PRI, they also can be can be held liable for money damages. This could include any profits they made utilizing PRI's information."

D. **Tortious Interference with Business Relations / Civil Conspiracy**

"I'd really like to sink these sea rats" Turner said. "Is there one more claim I might be able to bring?" Sparrow laughed, "How about two?"

"One potential claim against them would be for tortious interference with business relations. To prove such a claim, we would have to show (1) their acts were intentional and willful; (2) their acts were calculated to cause damage to PRI in its lawful business; (3) the acts were done with the unlawful purpose of causing damage and loss, without right or justifiable cause on the part of BPE or its President, and (4) actual damage and loss resulted."[41]

"In our case, I think we'll be able to prove all of that. First, their actions were clearly intentional and willful because we can show this scheme had been in the works for months. Second, their acts were calculated to cause damage to PRI, by taking away its business and customers using stolen information. Third, BPE has no lawful right to be using your information against you. Finally, we can show PRI has suffered actual damage because of their wrongful actions."

---

[41] *MBF* Corp. *v. Century Business Comm., Inc.*, 663 So.2d 595, 598 (Miss. 1995); *see also Accord McFadden v. U.S. Fidelity and Guaranty Co.*, 766 So.2d 20, 22-23 (Miss. App. 2000).

Sparrow continued, "Another possible claim would be for civil conspiracy. Conspiracy requires a finding of "(1) two or more persons or corporations; (2) an object to be accomplished; (3) a meeting of the minds on the object or course of action; (4) one or more unlawful overt acts; and (5) damages as the proximate result."[42] The purpose of the conspiracy has to be to accomplish an unlawful purpose or a lawful purpose unlawfully."[43]

"In your case, Barbossa, Teach, BPE, its President and your engineers had the goal of hurting PRI's business and clearly agreed on how they were going to go about it. Further, the unlawful acts involved the breach of fiduciary duty, violations of MUTSA and CFAA when they stole your information, as well as their tortious interference with your business relations."

VI. Conclusion

> Well, then, I confess, it is my intention to commandeer one of these ships, pick up a crew in Tortuga, raid, pillage, plunder and otherwise pilfer my weasely black guts out.
>
> ~ Captain Jack Sparrow

As illustrated by the fictional pirate tale above, dishonest employees rarely let you know in advance of their intention to "raid, pillage, plunder and otherwise pilfer" your company's trade secrets. However, employers who put in place the proper policies and practices are less likely to find themselves in the position of the overly trusting Will Turner, and better prepared for any legal battles against pirates and rogues in the workplace.

---

[42] *See Gallegos v. Mid-South Mortg. & Inv.*, Inc., 956 So.2d 1055 (Miss. App. 2007).
[43] *Mississippi Power & Light Co. v. Coldwater*, 106 So. 2d 375, 381 (Miss. 1958); *Shaw v. Burchfield*, 481 So. 2d 247 (Miss. 1985); 15A C.J.S. Conspiracy § 1(2).