This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

Hedge Fund Law Report
An Acuris company

High-Frequency Trading

When Must a Hedge Fund Manager (or Its Current or Former Employees) Preserve Evidence in Litigation or Potential Litigation Involving High-Frequency Trading Code?

Apr. 25, 2014

By Vincent Pitaro, *Hedge Fund Law Report*

Software is playing an increasingly central role in the investment processes of hedge funds, high frequency traders and other market participants. Most of the growing body of law around trading software focuses on who owns it, when it has been stolen and the remedies for theft. See "Recent Developments Affecting the Protection of Trade Secrets by Hedge Fund Managers," Hedge Fund Law Report, Vol. 6, No. 41 (Oct. 25, 2013). There is less law, and less commentary, on the application of civil procedure to trading technology disputes. Accordingly, a recent federal court decision is uniquely interesting to hedge fund managers and others that create and own trading technology; to technology and investment professionals that leave one shop to start another; and to lawyers and others professionally focused on intellectual property issues. A technology-based trading firm asked the court to impose spoliation sanctions on former employees who allegedly stole code from the firm, incorporated versions of that code into the trading technology of a new firm then – while aware of litigation involving the code – destroyed or erased various iterations of the code. In a carefully drafted opinion, the court applied the law of spoliation to this dispute involving trading software code. The court's opinion provides valuable guidance as to when, and to what extent, a duty to preserve electronic information pertaining to proprietary software exists and the criteria for imposing an appropriate sanction for spoliation.

Factual and Procedural Background

In 2009, Quantitative trading firms Quantlab Technologies Ltd. (BGI) and Quantlab Financial, LLC, (together, Quantlab) commenced this lawsuit in the U.S. District Court for the Southern District of Texas (Court) against former employees Vitaliy Godlevsky, Andriy Kuharsky, Anna Maravina and Ping An, competitor SXP Analytics, LLC (SXP), and SXP's founder Emmanuel Mamalakis. Quantlab alleged that the defendants had stolen or improperly used Quantlab's proprietary trading software.

In 2001, Quantlab hired Godlevsky and Kuharsky, who held Ph.D.'s in computational physics and applied mathematics, respectively. They worked as quantitative research scientists, writing code for the Quantlab trading system's "brain." Quantlab terminated their employment in 2007. Around that time, while spending time at an Arizona monastery, Godlevsky became acquainted

www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

with defendant Mamalakis, and the two began to discuss forming their own high-frequency trading firm. They were "inspired" by what Quantlab was doing, but testified that they had no intention of copying its trading practices: They merely desired to "build a better mousetrap."

In 2007, after terminating the employment of Godlevsky and Kuharsky, Quantlab sued them in Texas civil court to enjoin them from revealing Quantlab's trade secrets. It eventually discontinued that suit and brought suit in the Court. The suit was stayed while the U.S. Attorney considered whether to pursue criminal charges against Kuharsky and Godlevsky. The suit resumed after the U.S. Attorney declined to prosecute.

Aware of the litigation between Quantlab and Godlevsky and Kuharsky, Mamalakis formed high-frequency trading firm SXP in July 2007. Godlevsky and Kuharsky later joined SXP as principals and as part of its team of software engineers. Kuharsky left SXP in January 2008, taking with him all of the code he had written. In March 2008, the FBI raided the offices and homes of the three SXP principals. The Court's decision indicates that the FBI took all the principals' personal and business computer equipment, drives and related electronic equipment and recovered "hundreds of thousands of files that appeared to have been taken from Quantlab." SXP began operating again in the fall of 2008. Godlevsky left SXP in February 2011. Mamalakis decided to wind down the business in mid-2012. State and federal authorities have become more aggressive in treating alleged thefts of trade secrets as criminal matters.

Some time in 2012, Godlevsky reunited with Kuharsky and formed a new high-speed trading venture called Singletick. That firm is not a defendant in the Quantlab lawsuit, but Quantlab is seeking discovery from it, presumably to see if Kuharsky or Godlevsky used Quantlab code there.

Spoliation

The negligent or intentional destruction or alteration of evidence pertaining to a lawsuit is known as "spoliation." Routine destruction of documentation and electronically-stored information is generally permissible as long as the person in possession of that information is not under a duty to preserve it. A duty to preserve information arises when a person is a party to a lawsuit and knows that the information may be relevant to the lawsuit, or when a person has reason to believe that information in that person's possession may be relevant to future litigation. Under Rule 37 of the Federal Rules of Civil Procedure, a district court may impose a range of sanctions on a spoliator, including giving a jury instruction that entitles the jury to infer from the destruction of evidence that the evidence was unfavorable to the party that destroyed it (Spoliation Instruction), and even a so-called "death penalty" sanction – outright dismissal of the spoliator's case or entry of a judgment against the spoliator. Quantlab claimed that Mamalakis, Kuharsky and Godlevsky had spoliated evidence and asked the Court to impose "death penalty" sanctions on them. For the reasons discussed below, the Court did not believe that litigation-ending sanctions were warranted, but did conclude that those defendants had spoliated evidence and that Quantlab was entitled to a Spoliation Instruction.

Legal Standards

The Court explained that spoliation sanctions are imposed to remediate harm caused by the spoliation, to punish the spoliator and to deter future misconduct. In considering whether to impose a sanction for spoliation, a court will consider (i) whether there was a duty to preserve information; (ii) the culpability of the spoliator; (iii) the prejudice suffered by the opposing party;

www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

and (iv) which sanction is best suited to achieve the goals of remediation, punishment and deterrence. See "Employee Misappropriation of Trade Secrets Litigation Stresses Dangers of Willful Spoliation of Evidence; Texas Federal Court Orders Trial, Adverse Inference Instruction and Monetary Sanctions for Willful Destruction of Electronically Stored Information," Hedge Fund Law Report, Vol. 3, No. 11 (Mar. 18, 2010). A death penalty sanction is warranted when:

- The spoliator acted willfully or in bad faith.
- The litigant, as opposed to the litigant's attorney, destroyed the evidence.
- The spoliation prejudiced the opposing party. For prejudice to exist, the destroyed evidence had to be relevant to that party's claim or defense.
- A lesser sanction would not have a sufficient deterrent effect.

Quantlab did not allege that any of the defendants' attorneys was involved in the spoliation, so the Court did not address the second factor. The Court noted that bad faith is also a prerequisite to a Spoliation Instruction. Even negligent spoliation of evidence can lead to sanctions. See "*Pension Committee* Case Highlights Obligations of Hedge Fund Managers to Preserve Documents and Information in Anticipation of Litigation," Hedge Fund Law Report, Vol. 3, No. 6 (Feb. 11, 2010).

Analysis

Godlevsky, Kuharsky and Mamalakis all admitted that they had lost, destroyed or otherwise gotten rid of a great deal of their computer hardware and software. The Court considered, with respect to each of them, whether such person had a duty to preserve evidence, whether they acted in bad faith and whether the evidence was relevant to the suit (and therefore prejudicial to Quantlab). In all three cases, the Court found a duty to preserve, bad faith and relevance.

On the issue of the defendants' duty to preserve information, Quantlab argued that this suit was filed in 2009 and that Godlevsky and Kuharsky had been involved in litigation over Quantlab code since 2007. Quantlab had served discovery demands on Godlevsky, Kuharsky and Mamalakis in 2010, seeking to inspect their computers. Consequently, those defendants were on ample notice, at least since the commencement of this lawsuit, that Quantlab might want to inspect their computers. As for relevance, the crux of Quantlab's argument was that "each iteration of code written by Defendants since Dr. Kuharsky and Dr. Godlevsky departed from Quantlab's employ is relevant in determining whether that code was impermissibly based upon Quantlab's version." The Court largely accepted those arguments. It considered each defendant's actions separately:

Mamalakis

In 2012, while winding down SXP, Mamalakis "stored the company's servers and, after some deliberation, got rid of many of the individual developer workstations." He wiped clean or gave away 23 such workstations.

- *Duty*. Even though Quantlab did not specifically ask to inspect SXP's developer workstations, the breadth of its discovery demands was sufficient to give rise to a duty to preserve them: He "should have known that significantly altering or disposing of computers used by SXP employees was unwise."

www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

- *Bad Faith.* Mamalakis testified that he believed that SXP's servers contained all relevant information. However, he never told the Court that he planned to get rid of the workstations and made conflicting statements about whether and why he had done so. The Court found bad faith because he destroyed potential evidence three years into the litigation, concealed that destruction from the Court and made contradictory statements about his actions.
- *Relevance.* Mamalakis had preserved and delivered to Quantlab the final version of SXP's code. Quantlab's experts had shown that looking at the final version was insufficient to determine whether Quantlab's code had been used in developing the SXP code: It was necessary to view intermediate iterations of the code to see whether Quantlab code had been incorporated. The destroyed machines "would have provided a more complete picture of how SXP's code changed over time and could have helped to show whether SXP developers used Quantlab code as a guide while they worked."

Godlevsky

Quantlab's forensic expert had identified a host of external hard drives, thumb drives and other such devices that had been connected to Godlevsky's computers over time:

- 27 different devices that had been connected to the computers seized by the FBI in 2008, including computers that contained Quantlab code and/or on which Godlevsky had worked.
- 7 different devices that were connected to Godlevsky's computer in 2011 and 2012, including 2 that were also connected to a Singletick computer.
- 14 different devices that had been connected to Godlevsky's Singletick computer, 5 of which had also been connected to Kuharsky's computer.

Godlevsky produced only a single personal notebook computer and claimed he had lost or thrown away all of those external devices. He also admitted that he had not yet turned over a number of other computers and devices.

- *Duty.* Given that Godlevsky had already been sued by Quantlab in state court in 2007, he "should have known that litigation with Quantlab was likely enough that he could not treat potential evidence so carelessly." The 2008 FBI raid made that prospect even more obvious.
- *Bad Faith.* The Court reasoned that "the loss of a single device may well be the product of negligence, but a long-running inability to keep track of the tools of his trade seems more indicative of a reckless disregard for his obligations as a litigant and, more likely, bad faith." Even so, Quantlab did not produce any evidence that Godlevsky "acted with the express purpose of destroying evidence," so the Court could not conclude that he "acted with the most culpable state-of-mind possible."
- *Relevance.* The fact that Godlevsky worked as a software developer for Quantlab and moved on to other high-frequency trading businesses after he left made it likely that there was relevant information on the missing devices. The devices that were attached both to Godlevsky's computers and to those of Singletick "would be relevant in the sense that they could have helped to reveal whether Dr. Godlevsky has impermissibly used Quantlab code

www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

in more recent years." Those connected to both Quantlab and SXP computers would also have a "much higher likelihood of relevance."

Kuharsky

Quantlab alleged that Kuharsky had spoliated a number of flash drives, hard drives, encrypted storage devices, cloud-based storage sites and certain computers and other devices. It said that the FBI had seized "hundreds of thousands of Quantlab files from Kuharsky. . . ." As with Godlevsky, Quantlab's expert identified a great number of devices that Kuharsky may have used, among them:

- A flash drive plugged into Kuharsky's computer "at least 47 times" and from which a Quantlab file was downloaded onto an SXP computer, used for over 3 hours, and "accessed nearly simultaneously" with SXP programs.
- 27 different devices that had been connected to the computers seized by the FBI in 2008, including computers that contained Quantlab code and/or on which Kuharsky had worked.
- 2 devices that had been connected to Kuharsky's personal computer in 2013.
- Several "RAID" hard drives.

Kuharsky could not produce any of those devices. He said he had no recollection of the flash drive. He also indicated that he had taken the RAID drives apart, that he had lost or broken some devices and that he had given computers and other devices to family members in the Ukraine. He produced several encrypted drives but claimed that he had lost the passwords for them.

- *Duty.* Kuharsky's situation was similar to that of Godlevsky. Moreover, Kuharsky had told the FBI in 2008 that he had not deleted Quantlab code from his computer because he believed he was under a duty to preserve it.
- *Bad Faith.* The Court reasoned that "given that Dr. Kuharsky knew that he was obligated to preserve all potentially relevant evidence, it seems totally incomprehensible that he could have used a device some fifty times, and at least once for more than three hours, and then proceeded as if it did not exist. The same is true of a device he used in the summer of 2013. The Court feels it has no choice but to infer bad faith."
- *Relevance.* The devices that Kuharsky had failed to produce were "such obvious places to check for relevant evidence that the Court cannot possibly say it lacked relevance or that Quantlab was not prejudiced." As to Kuharsky's claims that the devices had nothing of value on them, the Court observed: "how easy it is for the one who lost the evidence to say that the evidence may not have been relevant."

In all three instances, the Court found bad faith, but was unable to conclude "with absolute certainty" that any defendant acted with the specific intent to destroy evidence. Similarly, without the missing computers and devices, it was impossible for the Court to know "with absolute certainty that the devices at issue would have proved useful at trial. But there seems a real possibility that they would have." Consequently, the Court concluded that, while litigation-ending sanctions were not warranted, a Spoliation Instruction was appropriate. However, the Court decided not to specify at this juncture how the Spoliation Instruction would be formulated. It would do so with the input of the parties and after "the nature of Quantlab's case

www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL

is brought into more crystalline focus, for doing so may shed new light on the relevance of the evidence lost."

Key Takeaways

The Court's decision provides several valuable lessons for persons or firms that are in possession of information that may be relevant to a pending or future lawsuit:

- A duty to preserve may exist even before the commencement of a lawsuit.
- A duty to preserve may exist even if a discovery demand does not reference a specific item of hardware or software.
- A belief that information is not relevant does not justify disposing of it.
- Where software is involved, it is not just the end product that is relevant: Intermediate iterations may show whether a third party's code has been incorporated.

To view the Court's Memorandum & Order, click here.

IMPORTANT: This article contains information protected by copyright which can only be used in accordance with the terms of your Hedge Fund Law Report subscription agreement. You must not therefore copy or forward this article, its contents, or any contents on the password-protected Hedge Fund Law Report website. (Your subscription agreement explains how you can use contents for reports and presentations.) UNAUTHORISED USE OR DISCLOSURE IS UNLAWFUL.

© 2019 Mergermarket Limited. All rights reserved.

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL