Computer Fraud and Abuse Act Limitations Accrued With Awareness of Unauthorized Access–Not Identity of Perpetrator

SUMMARY: The two year statute of limitations for Computer Fraud and Abuse Act claim began to run when the plaintiff had an awareness of an unauthorized access into its computer system even if the plaintiff did not know the identity of the alleged perpetrator at that time.

This is the second ruling on limitations issues in *Higgins v. NMI Enterprises, Inc.* In the earlier ruling, on January 2, 2013, the court granted a Motion to Dismiss certain Computer Fraud and Abuse Act (CFAA) claims based on when the Plaintiff "suspected" some sort of wrongdoing though the Plaintiff argued that "suspected" was not the same as "discovered." However, in making that ruling, the Court looked to facts outside of the pleadings by looking at a complaint filed in another matter. Because of that, the Court granted a Motion for Reconsideration and, pursuant to Rule 56(f)(3) notified the parties that it would consider summary judgment on its own.

The Latest Ruling in the Case

The citation for this new case is *Higgins v. NMI Enterprises, Inc.*, 2013 WL 4525635 (ED La. Aug. 26, 2013). The basic allegations are that a defendant had access to one of the plaintiff's e-mail password by virtue of his position in a related company, provided plaintiff's e-mail password to the other defendant's to read his e-mails to and from the other plaintiffs as well as those to and from his attorneys. On these allegations plaintiffs sued for violating the CFAA and the Wiretap Act on September 29, 2009.

The Issue: When Did Limitations Accrue?

The issue before the court was whether the claims were timely filed. The Computer Fraud and Abuse Act has a two year statute of limitations that runs from "the date of the act complained of or the date of the discovery of the damage." The evidence showed that, at least 2 years prior to September 29, 2009, the lead plaintiff knew *someone* had made an unauthorized access to the email account even though he only knew the IP address, not the actual identity of the alleged perpetrator. The plaintiff argued that the limitations period did not accrue until he discovered that person's actual identity.

The court disagreed and granted the Motion for Summary Judgment as to that defendant, reasoning as follows:

> *[U]nder [the Computer Fraud and Abuse Act], knowledge of unauthorized access is the information critical to begin the statute of limitation. There is no mention that a plaintiff must know the alleged perpetrator for the statute of limitations to begin. Unlike the plaintiffs in Quantlabb, here, Smith knew of the unauthorized access, even if he only suspected the identity of the perpetrator.*
>
> * * *
>
> *Thus, it is clear that Smith had an "awareness of an unauthorized access into [Thundervision's] computer system," which began the statute of limitations period more than two years before this action was filed.*

The court held that the two year statute of limitations for Computer Fraud and Abuse Act claim began to run when the plaintiff had an awareness of an unauthorized access into its computer system even if the plaintiff did not know the identity of the alleged perpetrator at that time. The court granted the Motion for Summary Judgment as to the primary plaintiff who had such knowledge, however, as to the remaining plaintiffs the court found there was a factual dispute issue as to when they had knowledge of the alleged unauthorized access and, therefore, did not grant summary judgment on their CFAA claims though it seemed to invite additional challenges to their CFAA claims as well.

Should you or anyone you know need assistance in dealing with possible claims under the Computer Fraud and Abuse Act or just want to talk about the law in general, please feel free to give me a call (469.635.1335) or email me (stuma@brittontuma.com) and I will be more than happy to speak with you.

Shawn E. Tuma
direct: 469.635.1335
stuma@brittontuma.com