INTRODUCTION TO COMPUTER SPOLIATION

This article reprinted with permission of Burke,
Warren, MacKay and Serritella, P.C.

February 2013 - Spoliation (spō-lē-ā-shen) is the destruction, alteration, or failure to preserve evidence. If a court determines that a party in litigation has failed to produce evidence due to spoliation, juries are instructed that they may infer that the evidence would be adverse so long as the evidence was: (a) under the control of the party that destroyed or altered it; (b) not equally available to the other party with the evidence; and (c) would have been produced by the party who destroyed the evidence if it was favorable. *Illinois Pattern Jury Instructions, Civil, No. 5.01.*

"A spoliation instruction is a powerful litigation tool that can be as damaging to your opponent as the evidence that was destroyed," said Gerry Ring, chair of the litigation group for Burke, Warren, MacKay & Serritella, P.C. Proving spoliation before computer forensics was difficult, and often required whistleblower testimony. Today, with the help of experts like Protek International, Inc.'s Keith Chval, spoliation can be easier to detect and prove at trial.

Keith is an attorney, former prosecutor and expert on the benefits, and limits, of digital investigation, including computer forensics. "Television shows like *CSI* create many myths about the ability to recover information that someone has intentionally tried to delete," said Keith, adding, "each investigation is unique and depends on the methods used to attempt to purge damaging evidence."

Protek's investigations can lead to conduct other than evidence destruction, including evidence manipulation. In one investigation, Protek identified the production of a "bogus" laptop computer in discovery. Upon its review of the computer that was produced, Protek learned that the emails it contained were created with Word 7 software. The problem for the party producing the computer, however, was that Word 7 software was never installed on it, so it could not have been the computer used to create the emails. Further investigation disclosed that the Word 7 emails on the bogus laptop had been transferred onto it from another computer via a USB port *after* the inspection was made - meaning the emails contained on the bogus laptop were cherry-

picked for the inspection, leaving the balance of the emails on the original computer that created them.

Unfortunately, software designed to destroy computer evidence continues to improve, making the destruction more common, and more challenging to detect. Keith advises clients that the best way to recover valuable evidence, or detect its destruction, is to act fast to preserve the evidence, and to protect the chain of custody to avoid inadvertent contamination to that it can be used at trial.