

**TENTH ANNUAL  
SOUTHERN SURETY AND FIDELITY CLAIMS  
CONFERENCE  
APRIL 15-16, 1999**

**DISCOVERY AND PROTECTION  
OF INSURANCE COMPANY DATABASES**

**PRESENTED BY:**

**DAVID T. KNIGHT  
LARA L. JONES  
HILL, WARD & HENDERSON, P.A.  
101 E. Kennedy Boulevard, Suite 3700  
Tampa, Florida 33602  
(813)221-3900**

# **DISCOVERY AND PROTECTION OF INSURANCE COMPANY DATABASES**

## **I. INTRODUCTION**

The discovery of insurance company databases is becoming one of the most hotly contested battles in insurance litigation. It is widely anticipated that the warfare over the discovery of these databases will grow increasingly fierce in the years to come. Today, attorneys representing insureds often request production of electronically stored information including e-mail, reserve information, and communication with reinsurers from insurance company computer systems. Are insurance companies required to produce this information? What steps should insurance companies take to protect these databases? These are some of the questions that will be addressed in this paper.

## **II. BACKGROUND**

Over the years, plaintiffs' attorneys have become increasingly aggressive during the discovery phase of litigation. Our highly computer literate society has brought about a new series of challenges to potential litigants. Today, computer databases have become indispensable in the corporate world and are used to organize and retain key information and documents. With increased frequency, however, attorneys for insureds are requesting potentially damaging information that is contained within these databases. In light of these challenges, companies must move from traditional document retention policies to disposal and retrieval policies for electronic communications. Although the discovery of insurance company databases is relatively new, it will continue to be an important issue in litigation. These databases are attractive to plaintiffs' attorneys because of the potentially damaging information stored within them -- information that could pose a serious threat to the defense of an insurance lawsuit.

## **III. DISCOVERABILITY OF INSURANCE DATABASES**

In federal courts, Federal Rules of Civil Procedure 26 and 34 govern the discovery of documents. Rule 26 was amended in 1993 to specifically require litigants to disclose all documents, including data compilations, that are relevant to disputed facts.<sup>1</sup> Data

---

<sup>1</sup> FRCP 26(a)(1)(B) provides, in pertinent part:

Initial Disclosures. Except to the extent otherwise stipulated or directed by order or local rule, the parties shall, without awaiting a discovery request, provide to other parties:

- B. A copy of, or description by category and location of, all documents, **data compilations** and tangible things in the possession, custody or control of the party that are relevant to disputed facts alleged with particularity in the pleadings. (Emphasis added.)

compilations include "computerized data and other electronically-recorded information."<sup>2</sup> In addition, under Federal Rule 34, any party may request -- and obtain -- documents stored on computer hard drives.<sup>3</sup> In fact, one court has observed that "[c]omputers have become so commonplace that most court battles now involve discovery of some computer-stored information." Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985). The Manual for Complex Litigation, for use in federal courts, recommends that "[a]t the outset of the litigation, the court should inquire into the existence of computerized data and processes for its retrieval."

As the rules now exist, it is not required that the computerized data be in comprehensible printed form, or even readily transformed into a comprehensible printed form. Discovery of information in the computer itself is permissible. Moreover, if a party provides a printout of data from this computer that is not in a computer-readable format, the court may well require the producing party to translate its data into a readable and useable form. See, e.g., National Union Electrical Corp. v. Matsushita, 494 F. Supp. 1257 (E.D. Pa. 1980).

Thus, absent computerized data that is privileged, a trade secret or otherwise protected from discovery by some traditional judicial doctrine, electronically stored information is discoverable. In instances where a privileged or other confidential status may attach to this information, a protective order under Federal Rule 26(c) or the equivalent state rule of procedure is available. One example where protective order protection should be available is the litigation support system used by clients and their counsel in litigation, at least to the extent necessary to protect the attorneys mental processes and litigation strategy. See, e.g., U.S. v. AT&T, 642 F.2d 1285 (D.C. Cir. 1980). These systems typically store deposition summaries, abstracts or imaging of important documents.

#### **IV. PROTECTION OF INSURANCE COMPANY DATABASES**

In light of the discovery challenges facing insurance companies in litigation, prudent insurers should take proactive measures to protect potentially damaging information. The best method by which insurance companies can protect this information is to create standard procedures to effectively shelter confidential and attorney-client privileged material from discovery. Insurers will want to protect as much information as possible, including e-mails, reserve information, communication with reinsurers and even corporate trash.

##### **a. E-mail**

Insurance companies have traditionally focused on document retention policies for the organization and storage of corporate documents. The increased use of computer technology requires that special procedures and policies must be implemented to provide for retention and disposal of electronic communications. Companies must also take special precautions to safeguard attorney-client privileged and confidential communications that are contained within e-mail.

---

<sup>2</sup> See Advisory Committee Notes to Rule 26.

<sup>3</sup> See Advisory Committee notes to Rule 34.

Insurance companies have a duty to preserve information that is relevant to ongoing or potential litigation.<sup>4</sup> Destruction of this information can give rise to (a) civil claims, such as spoliation; (b) judicial presumption against the party destroying the evidence; (c) ill will from the jury; and (d) possible criminal penalties. Generally, once an insurer is on notice of litigation, it must preserve its responsive electronic records. In order to comply with this requirement, insurers must first determine the point at which the obligation to preserve electronic information arises. Some courts have held that pre-litigation correspondence, acknowledging the future likelihood of litigation, is sufficient to impose a duty to preserve relevant documents.<sup>5</sup> For this reason, insurers must take an aggressive approach to preserve e-mail communications as soon as they become aware of even the potential for litigation.

In order to avoid spoliation issues, insurers should develop and disseminate e-mail policies to all of their employees. Many people who utilize e-mail believe that once an e-mail message is deleted, the message is removed from the computer hard drive. In reality, it is likely that the message has been stored by the computer onto the hard drive in a saved mailbox. Insurers need to create and enforce procedures to govern the use of e-mail systems, including a document retention policy. Most courts recognize that the intentional or negligent spoliation of evidence is unlawful. In the absence of a well-defined and consistently applied document retention policy, insurers who destroy computer records, including e-mail, run the risk of being sanctioned for spoliation of evidence.

Creating, implementing and maintaining an e-mail retention policy can be done with minimal effort. Insureds should keep in mind the following ideas when devising their own policies:

- Create a written policy.<sup>6</sup>
- Distribute the written policy to the entire staff, new hires, and periodically redistribute it.<sup>7</sup>
- Require employees to sign a release form signifying that they have read and understand the policy.<sup>8</sup>
- Restrict e-mail to be used for business purposes only.<sup>9</sup>
- Discuss with employees the sensitive nature of e-mail.
- Remind employees of the potential use of e-mail in litigation.

---

<sup>4</sup> Timothy Q. Delaney, *E-Mail Discovery - The Duties, Danger and Expense*, The Federal Lawyer, January 1999.

<sup>5</sup> William T. Thompson Co. v. Gen'l Nutrition Corp., 593 F.Supp. 1443, 1446 (C.D.Cal. 1984).

<sup>6</sup> Jill Hertz Ashman, *Slackers, Hackers, and Harassers Beware: E-Mail intensive litigation prompts corporate reforms*, Litigation News, January, 1999.

<sup>7</sup> John Araneo, *Pandora's (e-mail) Box: E-mail Monitoring in the Workplace*, 14 Hofstra Lab. L.J. 339, 362 (1996).

<sup>8</sup> Id.

<sup>9</sup> Ashman, *Supra* note 6

- Develop a warning message that will be displayed whenever a user logs on to the e-mail system.<sup>10</sup>
- When the retention period for a document expires and it is deleted from the database, make sure it is gone. This typically requires the additional step of purging the files.
- Provide passwords or encryption facilities to protect individual files.<sup>11</sup>

## **b. Reserve information**

Insurance companies often create a "loss reserve" when attempting to evaluate the potential loss that could be associated with a specific claim.<sup>12</sup> This reserve amount represents the amount of money that the insurance company may expect to pay as a result of the claim.<sup>13</sup> With increased frequency, insureds are seeking to discover the amount of the reserve that pertains to their claim.<sup>14</sup> If discovered, this information could seriously undermine the insurance company's settlement posture, and if admitted into evidence, it could seriously undermine the entire defense.

The most effective way for an insurer to protect this information is to shield it with an attorney-client or work product privilege.<sup>15</sup> An attorney-client or work product privilege will apply to prevent the discovery of reserve information as long as attorneys play a key role in the process of setting reserves.<sup>16</sup>

For the attorney-client privilege to apply, attorneys must have been involved in establishing reserves by preparing reports or documentation for use by the employees

---

<sup>10</sup>Kenneth S. Spierer, *Establishing an Electronic Communications Policy for a Broker-Dealer*, 1 No. 7 GLWSLAW 1, December 1997 suggests that a message could take the following form:

"You have accessed the [company name] electronic mail network. This network is to be used for business purposes only and not for personal use. Offensive, demeaning or disruptive messages are prohibited. All electronic communication through the network is the property of [company name] and is subject to supervisory review. Accordingly, you should have no expectations that your communications on these systems are private. Electronic communications should be treated with the same care as any other communication. Anyone who misuses company resources is subject to discipline, including immediate discharge."

<sup>11</sup> See Amy M. Fulmer Stevenson, *Making a Wrong Turn on the Information Superhighway: Electronic Mail, the Attorney-Client Privilege and Inadvertent Disclosure*, 26 Cap. U. L. Rev. 347, 512 (1977).

<sup>12</sup>Guy O. Kornblum, *Evidentiary Issues in Coverage and First-Party Bad Faith Cases*, 61 Def. Couns. J. 240, 246 (1994).

<sup>13</sup>Timothy M. Sukel and Mike F. Pipkin, *Discovery and Admissibility of Reserves*, 34 Tort & Ins. L.J. 191, 192 (1999).

<sup>14</sup>*Id.* at 191.

<sup>15</sup>*Id.* at 208.

<sup>16</sup>*Id.* at 209.

responsible for setting reserves.<sup>17</sup> For the work product doctrine to apply, attorneys must have been involved in the reserve setting process and the attorneys involvement must have taken place in anticipation of litigation with the insured.<sup>18</sup>

For either of these privileges to apply, insurance companies must create policies that require attorneys, whether in-house counsel or retained counsel, to take an active role in the reserve setting process. Insurers may want to consider requiring attorneys to complete thorough status reports once a claim is received. These status reports would allow the attorneys to place a subjective valuation on the claim prior to the reserve amount being set. The status reports should then be given to employees of the insurer to rely upon when establishing the reserve amount.

The increasingly controversial nature of pretrial discovery battles dictates that preventative measures must be taken by prudent insurers to protect reserve information. Although requiring attorneys to be actively involved from the onset of a claim may seem burdensome, these steps will prevent insurers from compromising the defense of lawsuits.

### **c. Communication with reinsurers**

Once insurers successfully clothe reserve information and privileged material with the attorney-client or work product privilege, it is important to ensure that the privilege is not waived through communication with reinsurers. Clever attorneys who represent insureds may assert that communication between the insurer and a reinsurer waives the privilege that would otherwise apply to protect this information from discovery. Generally, voluntary disclosure of privileged information results in waiver of the privilege.<sup>19</sup> In order to avoid waiver, insurers must show that a common interest exists between the insurer and the reinsurer.<sup>20</sup> The common interest doctrine may be successfully asserted when different persons or corporations have an identical legal interest with respect to the subject matter of a communication between an attorney and a client concerning legal advice.<sup>21</sup>

Insurers and their reinsurers share a common interest in the successful resolution of pending litigation by insureds.<sup>22</sup> As a practical matter, insurers and their reinsurers must be able to communicate concerning pending claims without fearing that these communications

---

<sup>17</sup> Id. at 208.

<sup>18</sup> Id.

<sup>19</sup> Id. @ 213, citing In Re: Horowitz, 482 F.2d 72, 81 (2nd Cir.), cert. den'd, 414 U.S. 867 (1973); United States v. Aronoff, 466 F.Supp. 855, 862 (S.D.N.Y. 1979); Durham Indus., Inc. v. North River Ins. Co., No. 79 Civ. 1705, 1980 W.L. 112701 (S.D.N.Y. Nov. 21, 1980).

<sup>20</sup> Id.

<sup>21</sup> Id. citing DuPlan Corp. v. Deering Milliken, Inc., 397 F.Supp. 1146, 1172 (D.S.C. 1974).

<sup>22</sup> Id. @ 214

will be disclosed to insureds.<sup>23</sup> To protect this information, insurance companies and their reinsurers should be cautious about the nature and content of their communications.

Courts are more likely to hold that an insurer and its reinsurer share a common interest worthy of protection in the context of impending or anticipated litigation<sup>24</sup>. For this reason, communications that occur prior to the anticipation of litigation are not guaranteed protection through the attorney-client or work product privilege. As a result, insurers must be very careful when communicating with reinsurers prior to the onset of a lawsuit. Pre-litigation correspondence should not contain any information that the insurer would not want the insured to discover.

As an extra precaution once litigation ensues, insurance companies and their reinsurers should allow attorneys to handle as much of their communication as possible. Also, they should create disclaimers to notify unintended recipients that the information contained within correspondence are subject to the attorney-client privilege.<sup>25</sup> Although valid disclaimers will not completely ensure the protection of privileged material, it will help support the argument that a privilege exists.

#### **d. Corporate Trash**

Desperate plaintiffs have been known to take drastic measures in an attempt to uncover confidential material. A recent article by Jerold S. Solovy and Robert L. Byman titled *Fighting Those Who Dive Into High-Tech Dumpsters*,<sup>26</sup> discusses a new low reached by plaintiffs known as “dumpster diving”. These desperate measures pose new responsibilities on defendants -- protecting their trash.<sup>27</sup>

In *Suburban Sew N’ Sweep, Inc. v. Swiss-Bernina, Inc.*, 91 F.R.D. 254 (N.D. Ill. 1981), the president of Swiss-Bernina disposed of hand-written drafts of attorney-client privileged letters in his wastebasket. The drafts were discarded into a trash dumpster used solely by Swiss-Bernina. The plaintiffs entered Swiss-Bernina property without permission, searched

---

<sup>23</sup> Id.

<sup>24</sup> See Id. @ 216.

<sup>25</sup> Typical disclaimers contain information similar to the following:

This message is intended only for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us at the above address via the U.S. Postal Service.

<sup>26</sup> THE NATIONAL LAW JOURNAL, December 21, 1998.

<sup>27</sup> Id.

through the trash dumpster, and located the otherwise privileged drafts. The magistrate judge ordered the documents be returned to Swiss-Bernina. The district judge reversed, finding that Swiss-Bernina had waived the privilege by failing to take better precautions.<sup>28</sup>

The result reached by the court in *Sew N' Sweep* dictates that insurance companies take special precautions to protect confidential material contained within corporate trash. Companies should shred all garbage that contains attorney-client and confidential information.<sup>29</sup> Also, these policies must be applied to computer technology. Electronic communications must be protected from computer hackers that pose a similar threat as dumpster divers.<sup>30</sup>

## V. ETHICAL ISSUES FOR ATTORNEYS

Both outside and in-house counsel for insurance companies are required to observe the various ethical rules which govern their legal work. One of the most sacred rules governing the lawyer/client relationship is that a lawyer will protect the confidences of his client. The American Bar Association has promulgated Model Rules of Professional Conduct. Model Rule 1.6(a) provides that a "lawyer shall not reveal information relating to the representation of a client unless the client consents after consultation . . ." This rule, requiring a lawyer to preserve the confidences of the client, is found in one form or another in all of the ethical codes for lawyers. See e.g. Rule 4-1.6 of the Rules Regulating the Florida Bar which is virtually identical to the ABA Model Rule.

Applied to computer databases, it is generally observed that this duty of the lawyer requires him to take reasonable steps to insure that information on his computer is adequately protected from unauthorized disclosure. So, in addition to risking a crippling injury to the client's case by accidental disclosure of privileged or confidential information, the outside or inside attorney that does not adequately protect his database may potentially be subjected to ethical sanctions.

---

<sup>28</sup> But see, *McCafferty's, Inc. v. Bank of Glen Burnie*, 179 F.R.D. 163 (D. Md. 1998).

<sup>29</sup> Solovy and Byman, *Supra* note 22.

<sup>30</sup> Id.