THE ELECTRONIC COMMERCE SECURITY ACT

A new method of conducting business begins in Illinois on July 1, 1999. That is the date on which The Electronic Commerce Security Act (the ECSA) becomes effective. The ECSA will surely spur electronic commerce and propel us further into the Digital Age.

Like almost all other aspects of our society, the law is having trouble keeping up with the rapid changes in technology. Until now, this was especially true when it came to contracts. Most states, including Illinois, have an ancient law known as the Statute of Frauds, which provides that contracts are not enforceable unless they are "signed" and "in writing." This archaic law raises a significant barrier to electronic commerce. According to the Statute of Frauds, agreements entered into entirely electronically (i.e., by email, through the Web, or by other electronic media) are neither signed nor written. Therefore, they may be unenforceable.

The ECSA overrides the Statute of Frauds in two important respects. *Electronic records*, which are information transmitted by and stored within computers, now satisfy the requirement of a writing. *Electronic signatures,* which are symbols (letters, numbers, etc.) generated by a computer that are intended to authenticate an electronic record, now satisfy the requirement of a signature.

Until recently, the veracity and security of electronic records presented as big a barrier to electronic commerce as did the law. The ECSA takes this into account through a provision in the stature called *qualified security procedures.* By means of qualified security procedures, parties engaged in electronic commerce are assured that their electronic records (such as their contracts) and their electronic signatures are valid and secure.

The ECSA provides for two types of qualified security procedures, namely; any procedure that the parties have agreed to use (such a private escrow agent who hold the electronic records in its server) and any procedure certified by the Illinois Secretary of State (of which there are presently none). The ECSA also provides for two procedures to verify electronic signatures, which are once again any procedure to which the parties have agreed (such as using commercially available encryption software) and any procedure certified by the Secretary of State (again, of which there are presently none).

If parties agree on the procedures to verify and secure their records or their signatures, under the ECSA they will be obliged to use reasonable care to prevent the unauthorized use of those procedures. Absent such reasonable

care, the use of those procedures by innocent third parties may be binding on whomever failed to use the proper care.

As noted above, electronic signatures will probably be a string of letters, numbers, and other symbols rather than a copy of your handwritten signature. This string may be accessible only by, for example, the use of a secret password. If you carelessly enable an unauthorized person to gain access to that password, who then uses it to purchase merchandise, you may be obliged to pay the vendor who innocently relied on the password even if you never received the goods.

The ECSA represents yet another step down the information superhighway. The way in which the world is conducting business is dramatically changing. Business owners will either adapt to those changes or disappear like the dinosaurs and buggy whip manufacturers.