

VIRGINIA BUSINESS TORTS

VIRGINIA CLE

Virginia Computer Crimes Act

Milton Babirak, Esquire
Babirak, Vangellow & Carr, P.C.
47539 Coldspring Place
Sterling, Virginia 20165
703.406.4600
mbabirak@bvcpc.com
www.bvcpc.com

Virginia Computer Crimes Act

Table of Contents

- I. INTRODUCTION**
- II. VIRGINIA COMPUTER CRIMES**
- III. OTHER PROVISIONS OF THE ACT**
- IV. CONCLUSION**

Virginia Computer Crimes Act

Milton E. Babirak, Jr.¹
Babirak, Vangellow & Carr, P.C.
Sterling, Virginia

I. Introduction

The Virginia Computer Crimes Act (“Act”) became effective July 1, 1984. It was amended and supplemented on several occasions.² Several other states have enacted computer assisted crime legislation.³

One of the reasons for this legislation was the controversial 1977 case of *Lund v. Commonwealth*,⁴ when the Virginia Supreme Court held that unauthorized use of computer time and services could not constitute either grand larceny or false pretenses under existing Virginia statutes because computer time and services were not “property.” The General Assembly immediately responded to the decision and in 1978 enacted a statute that made computer time and services property for such purposes. In 1984, after reviewing several bills designed to expand the coverage of the 1978 statute, the General Assembly created and passed the completely revised Virginia Computer Crimes Act (“Act”).⁵ The old legislation which was located in Virginia Code section 18.2-98.1 was repealed and replaced by fourteen new sections, 18.2-152.1 through 18.2-152.14. The Act consisted of an extensive set of definitions, and specified the elements of five new computer crimes: computer fraud, computer trespass,

¹ The author of this document is not a criminal law practitioner. This document is drafted as a potential aid to the Virginia civil litigator who may be seeking damages or other civil relief for his or her client pursuant to the Act. Phone: 703.406.4600; Email: mbabirak@bvcpc.com.

²For a description of the history of the Act, see Daniel R. Burk, *Virginia’s Response to Computer Abuses: An Act in Five Crimes*, 19 Univ. Rich. L.R. 85, 85-96.

³ For some statistics concerning such state legislation, see Robin K. Kutz, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 Wm. & Mary L. Rev. 783, 789 (Summer, 1986).

⁴ 217 Va. 688, 232 S.E.2d 745 (1977).

⁵ Va. Code Ann. Code Sections 18.2-152.1 to 152.15

computer invasion of privacy, theft of computer services and personal trespass by computer. The original Act also makes it clear that embezzlement includes the embezzlement of computer time and services. As supplemented, the Act now provides for other crimes as well as described herein. (A copy of the current Act is attached as Exhibit 1.)

The Act is a criminal statute. However and significantly, the Act also provides for civil relief for damages, costs, lost profits and any additional civil remedy otherwise allowed by law⁶ in the case where any person is injured by reason of a violation of any provision of the Act. The review and analysis of this Act herein is intended for the Virginia attorney who is a civil litigator. This review of the Act was not from the perspective of or for a criminal practitioner.

The nature and structure of this private right of action provision in the Act is similar in nature to the criminal Virginia Business Conspiracy Statute⁷ which prohibits two or more people from combining to willfully and maliciously injure another in his reputation, trade, business or profession.⁸ This Virginia Business Conspiracy Statute permits a person who has been so injured to sue for treble damages, costs, lost profits and attorney's fees.⁹ While the Virginia Computer Crimes Act does not provide for treble damages or attorney's fees, the structure of and civil relief otherwise described in the Virginia Computer Crimes Act is similar to that of the Virginia Business Conspiracy Statute.

Punitive damages are not permitted by the Act.¹⁰ While the Act does not contain a provision specifically permitting an injunction as a remedy, one commentator concluded that such a remedy would "...always be available in appropriate circumstances."¹¹

⁶ Section 18.2-152.12.A. and F.

⁷ Va. Code Section 18.2- 499 *et. seq.*

⁸ There is a very interesting and useful Virginia article on this cause of action recently published at: J. Scott Sexton, *What's In A Word? The Tortured Life of the Virginia Conspiracy Statute*, VA Code Sections 18.2-499 and -500, Litigation News, VSB, Vol. XI, Number 1, Spring 2004.

⁹ Va. Code Section 18.2- 500.

¹⁰ *McGladrey & Pullen, L.L.P. v. Shrader*, 62 Va. Cir. 401, 2003 Va. Cir. LEXIS 274 (Rockingham County 2003).

II. Virginia Computer Crimes

Computer Fraud. The first cause of action set forth in the Act is for computer fraud.¹² The Act describes this cause of action as: Any person who uses a computer or computer network without authority and with intent to: (i) obtain property or services by false pretenses; (ii) embezzle or commit larceny; or (iii) convert property of another is guilty of the crime of computer fraud. The crime of computer fraud is punishable as a Class 5 felony if the value of the property or services is \$200 or more. If the value is less, it is a Class 1 misdemeanor.

The private right of action for computer fraud¹³ was one of the seven counts alleged in *America Online, Inc. v. LCGM, Inc.*¹⁴ Plaintiff AOL complained that the defendants sent large numbers of unauthorized and unsolicited bulk e-mail advertising pornographic web sites to its members. Defendants admitted to causing “aol.com” to appear on electronic header information of email messages which they sent to AOL members. Plaintiff alleged that the Defendants intended to obtain services by false pretenses and to convert AOL’s property. Plaintiff also alleged that Defendants illegally obtained the use of AOL’s email delivery service and obtained free advertising from AOL because AOL bore the cost of sending the messages. The Court granted AOL’s Motion for Summary Judgment, finding there were no genuine issues for trial.

In *Physicians Interactive v. Lathian Sys.*,¹⁵ the Plaintiff successfully brought a private right of action under the Act for computer fraud. In this case, Plaintiff, a website host, argued that a competitor and its employee obtained its property by false pretenses. Plaintiff alleged that the competitor and its employee hacked into Plaintiff’s computer but could not prove what

¹¹ Daniel R. Burk, *Virginia’s Response to Computer Abuses: An Act in Five Crimes*, 19 Univ. Rich. L.R. 85, 85-96.

¹² Va. Code Ann. Section 18.2-152.3.

¹³ See *Rosciszewski v. Arete Associates, Inc.*, 1 F.3d 225 (4th Cir. 1993).

¹⁴ 46 F.Supp.2d 444 (E.D. Va. 1998).

¹⁵ ---F.Supp.2d---, 2003 U.S. Dist. LEXIS 22868 (E.D. Va. Dec. 5, 2003).

Defendant did after that. The Court found that it was highly likely that the Defendants converted Plaintiff's proprietary information for their own use.

In a Rockingham County Circuit Court decision of *McGladrey & Pullen, L.L.P. v. Shrader*,¹⁶ computer fraud was again at issue. Therein, a Defendant employee filed a demurrer claiming he had authority to use his employer's computer and to download certain data. The Circuit Court overruled the demurrer, finding Defendant had no authority to use his employer's computers for purposes not authorized by his employer and inimical to his employer's best interest.

Transmission of unsolicited bulk electronic mail. The second crime set forth in the Act is the transmission of unsolicited bulk electronic mail,¹⁷ commonly referred to as "spam." The elements of this cause of action may be summarized:

Any person who:

1. Uses a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of UBE through or into the computer network of an electronic mail service provider or its subscribers; or
2. Knowingly sells, gives, or otherwise distributes or possesses with the intent to sell, give, or distribute software that;
 - (i) Facilitates or enables falsification of e-mail transmission or other routing information;
 - (ii) Has only limited commercial purpose or use; or
 - (iii) Is marketed for such purpose or use.

This crime is a Class 1 misdemeanor. It is a Class 6 felony if: (1) the UBE transmitted is over 10,000 attempted recipients in 24 hours, 100,000 attempted recipients in 30 days or one million attempted recipients in one year, or (2) the revenue generated from a specific UBE transmission exceeds \$1,000 or the total revenue generated from all UBE to any electronic mail service provider exceeds \$50,000. It is a Class 6 felony to hire, employ, use or permit any minor to assist in the transmission of UBE in violation of (1) and (2).

¹⁶ 62 Va. Cir. 401, 2003 Va. Cir. LEXIS 274 (Rockingham County 2003).

¹⁷ Va. Code Ann. Section 18.2-152.3:1.

In addition to these statutory provisions, several courts, including the US District Court for the Eastern District of Virginia, have held that under certain circumstances, the transmission of UBE through a computer system constitutes the tort of trespass to chattel.¹⁸

In the case of *Verizon Online Services, Inc. v. Ralsky*,¹⁹ Plaintiff Verizon, a Virginia resident, sued Defendants, Michigan residents, based on their alleged transmission of millions of UBE to Verizon's subscribers through Verizon's on-line proprietary network of seven e-mail servers located in Virginia. In its Amended Complaint, Verizon alleges three counts under the Virginia Act and other statutory and common law counts. Defendants moved for dismissal for lack of personal jurisdiction under Rule 12(b) (2) of the Federal Rules of Civil Procedure and improper venue or sought to have the matter transferred to the Eastern District of Michigan, the location of the Defendants. The Court denied the motions finding that the Defendants transmission of millions of pieces of UBE to and through Plaintiff's servers in Virginia constituted sufficient minimum contacts to satisfy the demands of the Due Process Clause of the Fourteenth Amendment of the Constitution.

In *Commonwealth v. Jaynes*,²⁰ the Defendants were charged with felony violations of the Act for the transmission of UBE to American Online and its subscribers. Defendants filed several motions to dismiss challenging the statute on constitutional grounds, suggesting that section 18.2-152.3:1 violated the First Amendment protection of free speech, contravened due process protection against vagueness, and was inconsistent with the Commerce Clause. The Court denied these motions and found that the Act prohibited unauthorized routing of UBE rather than UBE content, and therefore did not implicate the First Amendment, nor was the Act found to be vague or offensive to interstate commerce.

¹⁸ See *America Online v. LCGM*, 46 F. Supp. 2d 444, 451-52 (E.D. Va. 1998); *Hotmail Corp. v. Van\$ Money Pie, Inc.*, 47 U.S.P.Q. 2d 1020, 1022 (N.D. Cal. 1998); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1018 (S.D. Ohio 1997).

¹⁹ 203 F. Supp. 2d 601 (E.D. Va. 2002).

²⁰ 65 Va. Cir. 355 (Va. Cir. Ct. 2004).

The US District Court of the Eastern District of Virginia has decided several cases involving American Online as Plaintiff and has consistently held that the practice of sending UBE, unauthorized by AOL, and using techniques to evade AOL's blocking mechanisms violates the Act.²¹ In the recent case of *American Online v. Smith*,²² the Defendant transmitted billions of UBE messages to Plaintiff's subscribers on a daily basis for a period of 213 days, using numerous fraudulent and deceptive methods to evade Plaintiff's e-mail filters and disrupt its business operations. The Court granted Plaintiff's summary judgment motion, and awarded \$25,000 per day for each of the 213 days that a violation took place, and attorney's fees and costs.²³

The Act also provides a civil remedy for the recipient of unsolicited bulk electronic mail ("UBE") who is injured by UBE sent by another (not the electronic mail service provider ("EMSP")). Such an injured party may recover attorney's fees and costs and receive as damages in the amount of the lesser of \$10 for each UBE email or \$25,000 per day in lieu of actual damages.²⁴ The Act also provides that the EMSP may recover attorney fees and costs from the spammer and, in lieu of actual damages, \$1.00 for each UBE or \$25,000 per day.²⁵ These provisions do not apply to the transmission of email by an organization to its members.

Computer trespass. The crime of "computer trespass²⁶" actually covers six different activities, all involving any person who uses a computer or computer network without authority and with the intent to do one of the following:

²¹ See *American Online, Inc. v. CN Prods.*, 272 B.R. 879 (E.D. Va. 2002); *American Online, Inc., v. GreatDeals.Net*, 49 F. Supp. 2d 851 (E.D. Va. 1999); *American Online, Inc., v. Prime Data Sys.*, 1998 U.S. Dist. LEXIS 20226 (E.D. Va. 1998); *American Online, Inc. v. LCGM, Inc.*, 46 F. Supp 2d 444 (E.D. Va. 1998); *American Online, Inc. v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998).

²² 2006 U.S. Dist. LEXIS 4813 (E.D. Va. 2006).

²³ Va. Code Section 18.2- 152.12.C.

²⁴ Va. Code Section 18.2- 152.12.C.

²⁵ *Id.*

²⁶ Va. Code Ann. Section 18.2-152.4.

- (1) Temporarily or permanently remove, halt or otherwise disable any computer data, programs, or computer software²⁷;
- (2) Cause a computer to malfunction;
- (3) Alter or erase any computer data, programs or software;
- (4) Effect the creation or alteration of a financial instrument or electronic transfer of funds;
- (5) Cause physical injury to the property of another; or
- (6) Make an unauthorized copy of any computer data, program or software residing in, communicated by or produced by a computer or computer network.

Of course, the common thread amongst these six crimes of computer trespass is that the object of the criminal activity is the computer data or the computer itself. The statute specifically provides for two interesting exceptions to the criminal characterization of the six activities prohibited by this section of the Act. First, a Virginia-based ISP can enter into contracts or licenses or implement technical measures which might otherwise violate the statute in order to prevent UBE. Also, this section does not prohibit a parent or guardian from monitoring of a minor's computer usage.

Computer trespass is a Class 1 misdemeanor. However, if there is damage to property valued at \$2,500 or more and is caused by a malicious act, the offense is a Class 6 felony.

With regard to the first crime set forth in this section, to temporarily or permanently remove, halt or otherwise disable any computer data, programs, or computer software, there is a substantial similarity between this crime and the crime described in the Act as computer fraud. Both concern the taking of computer property; however, there are some important differences²⁸. In computer

²⁷ *O'Conner v. Commonwealth*, 16 Va. App. 416, 430 S.E.2d 567 (1993), documents are not "computer software."

²⁸ For a more complete discussion of this topic, see Robin K. Kutz, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 Wm. & Mary L. Rev. 783, 823 *et seq.* (Summer, 1986).

trespass, the focus is on computer data, programs and computer software. In computer fraud, the crime can involve any property or services. Secondly, in computer trespass cases, only a temporary taking of the property is required. In computer fraud by larceny, false pretenses, embezzlement or conversion, the defendant must have intended to deprive the owner of his property permanently.

The second crime set forth in this section, to cause a computer to malfunction, may also constitute another Virginia crime, malicious mischief.²⁹ Under the Virginia malicious mischief statute, any person who unlawfully destroys, defaces, damages or removes, without intent to steal, any property not his own, is guilty of malicious mischief.

Computer invasion of privacy. The crime of computer evasion of privacy³⁰ is committed when any person uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. “Examination” in this context means the offender reviewed the information after the time at which the offender knows or should know that he is without authority to view the information. The crime is a Class 1 misdemeanor.

The private right to civil relief for damages caused by this crime was at issue in the 1999 case of *S.R. v. Inova Healthcare Services*.³¹ Plaintiff was a healthcare professional employed at Fairfax Hospital. She sought psychiatric treatment at Alexandria Hospital so her co-workers at Fairfax Hospital would not know of her illness or treatment. Employees of Fairfax Hospital used a computer at that Hospital to access her medical records at Alexandria Hospital including her admitting medical condition. The Plaintiff sued both Fairfax and Alexandria Hospitals, INOVA Healthcare Services, two nurses and others. The Court found that the delineation of the elements

²⁹ Va. Code Section 18.2-137.

³⁰ Va. Code Ann. Section 18.2-152.5; *Plasters v. Commonwealth*, No. 1870-99-3, 2000 Va. App. LEXIS 473 (Va. App. 6/27/00), criminal conviction for computer invasion of privacy.

³¹ 49 Va. Cir. 119, 1999 Va. Cir. LEXIS 287 (Fairfax County Cir. Ct. 6/1/99).

of this statutory cause of action was a matter of first impression in Virginia³². Defendants demurred, arguing *inter alia* that Plaintiff's claim rests on the incorrect assumption that a hospital is without authority to view the records of its patients. The court held that a "...plain meaning analysis of this statute reveals that its enactment was not aimed at preventing hospitals or other enterprises from accessing confidential information necessary to effectively conduct business. Rather, the statute is aimed at preventing the unauthorized examination of personal information." The Court noted that, while the statute does not specifically prohibit the examination of medical information, it does specifically refer to personal information. The Court found that personal information may include medical information. In reaching this later finding, the Court cited a seminal Virginia law review article on this topic.³³

There are two notable aspects to this crime. First, it is the examination itself that is unlawful. The offender does not have to use or disclose the prescribed information. In a sense this type of information is treated in a fashion similar to a trade secret under the Virginia Uniform Trade Secret Act where the mere wrongful acquisition of a trade secret is a misappropriation.³⁴ A trade secret may be misappropriated without being used or disclosed. The statute also clearly requires that any examination of the prescribed information must be intentional. From a policy point of view this makes a great deal of sense, however, this may present substantial problems of proof in some cases.

Theft of computer services. Naturally, the Act also prohibits the theft of computer services.³⁵ Any person who willfully uses a computer or computer network with intent to obtain computer services without authority commits the crime of theft of computer services. The crime is a Class 1 misdemeanor. If the theft is of services valued at \$2,500 or more, it is a Class 6 felony.

³² *Id.*

³³ Robin K. Kutz, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 Wm. & Mary L. Rev. 783, 823 *et seq.* (Summer, 1986).

³⁴ Va. Code Ann. §§ 59.1-336 (Michie 2000).

³⁵ Va. Code Ann. Section 18.2-152.6.

If the willfulness requirement of the statute were to be interpreted literally, this statute would criminalize the commonplace activities of many employees who use their employer's computer at work to keep a personal calendar, send an email a friend, or check the weather or traffic on the Internet. Certainly, the scope of this statute is not intended to be so broad. Not all such uses of computer services should be treated as a theft. In most cases, it is appropriate and sufficient to resolve the use and misuse of employers' computers and Internet access in the context of employer disciplinary procedures. Employers frequently publish general guidelines in their employment handbooks or manuals or they publish acceptable computer and Internet use programs, therein setting forth what is acceptable computer and Internet use in the employment context.

The statutory language requirement of "willfulness" in the crime of theft of computer services should be read in the context of Virginia case law. The measure and scope of "willfulness" in a criminal statute has been frequently defined by Virginia case law. For example, in the case of *United States v. Adair*, decided by the U.S. District Court of the Western District of Virginia,³⁶ the Court held that the Defendant's threatening actions were willful because the Defendant comprehended his action, and deliberately, voluntarily, and intentionally acted. In *Omega World Travel, Inc., v. Omega Travel, Inc.*,³⁷ the Court defined willfulness as obstinate or recalcitrant conduct, and held that the Defendant's neglectful and careless actions in disregard of a court order did not rise to this level of willfulness. In *United States v. Frazier*,³⁸ the Defendant's actions rose to the level of willfulness because her spending activities were in reckless disregard of a known risk that her taxes were not paid. In *Reed v. Commonwealth*,³⁹ the Court found that the Defendant did not violate the criminal trespass statute which required a willful trespass because he trespassed in good faith with an actual and sincere belief that he was authorized to do the act in question.

³⁶ 227 F. Supp. 2d 586, 591 (W.D. Va. 2002).

³⁷ 710 F. Supp. 169, 173 (E.D. Va. 1989).

³⁸ 1989 U.S. Dist. LEXIS 9719 (W.D. Va. 1989).

³⁹ 6 Va. App. 65 (Va. Ct. App. 1988).

Personal trespass by computer. A person is guilty of the crime of personal trespass by computer if he uses a computer or computer network without authority and with the intent to cause physical injury to an individual.⁴⁰ A few simple examples of such a crime might involve the use of a computer or computer network to interfere with traffic lights, electricity or other utilities. More complex examples might be the destruction of patient or even research computer data used by a hospital or healthcare provider. The statute provides that the crime is a felony; if it is committed maliciously, it is a Class 3 felony and if it is committed unlawfully but not maliciously, it is a Class 6 felony.

For this crime, the Act only requires an “...intent to cause physical injury...” and, accordingly, is similar in nature to an assault. The Virginia statute on assault and battery⁴¹ makes a simple assault or assault and battery a Class 1 misdemeanor. (If the assault and battery is against a person because of his race, religious conviction, color, national origin, law enforcement officer, correctional officer and other defined persons, it is a Class 6 felony.⁴²) Accordingly, if a simple assault is committed using a computer or computer network, it’s a felony. If a simple assault or even a simple assault and battery is committed but there is no use of a computer or computer network, it’s a misdemeanor. While this difference may be significant to a criminal law practitioner, it may not have much relevance to plaintiff’s counsel seeking damages in a civil action. Of course in such a case, the civil lawyer will still have to prove the measure of damages.

Harassment by computer. Any person who, with the intent to coerce, intimidate, or harass any person, shall use a computer or computer network to communicate obscene, vulgar, profane, lewd, lascivious or indecent language, or make any suggestion or proposal of an obscene nature

⁴⁰ Va. Code Ann. Section 18.2-152.7.

⁴¹ Va. Code Ann. Section 18.2-57.A.

⁴² Va. Code Ann. Section 18.2-57.B. and C.

or threaten any illegal or immoral act, commits the crime of harassment by computer.⁴³ It is a Class 1 misdemeanor.

Perhaps it is not an exaggeration to say that anyone who has a computer has received an email, frequently from someone they know, which communicates such language, suggestion, proposal or threat. Arguably, those still-too-common emails advertising sexual performance enhancing drugs or medications may be considered by some as a proposal of an obscene nature. Off-color jokes sent by email by co-workers or friends may contain language that is obscene, vulgar, profane, lewd, lascivious or indecent. However, in order for these communications to be criminal under this statute, the intent of the person using the computer or computer network must be to coerce, intimidate, or harass.

There is a logical but incomplete connection between the crime of harassment by computer and the crime of personal trespass by computer. The crime of personal trespass by computer requires intent to cause physical injury to a person. The crime of harassment by computer proscribes certain acts committed with the intent to coerce, intimidate, or harass. Of course in many cases, such coercion, intimidation and harassment may amount to the expression of an intent to cause physical injury to a person. For example, a suggestion or proposal of an obscene nature or threat of an illegal or immoral act may be the expression of intent to cause physical injury.

A significant difference between the two crimes is the nature of the injury in each case. While this may be obvious, it is important because it influences the nature of the proof of damages and the amount of damages that may be recovered. In the case of personal trespass by computer, the injury arises out of an expression of an intent to cause physical injury to a person. In the case of the crime of harassment by computer, it arises out of an intent to coerce, intimidate, or harass. The injury, and therefore the damages, may be a lot easier to prove in the case of physical injury than in the case of coercion, intimidation and harassment. This is not to say that substantial damages can not be proven in coercion, intimidation and harassment cases but proving the damages will obviously be different than physical injury cases and possibly more difficult.

⁴³ Va. Code Ann. Section 18.2-152.7:1.

Property capable of embezzlement.⁴⁴ The embezzlement statute in the Virginia Code⁴⁵ specifically itemizes the property that may be the subject of embezzlement such as money, bill, note, check, order, etc. In 1977 in *Lund v. Commonwealth*,⁴⁶ the Virginia Supreme Court held that unauthorized use of computer time and services could not constitute either grand larceny or false pretenses under the existing Virginia embezzlement statute because computer time and services were not listed therein as “property.” The then current embezzlement statute did not list computers or computer services. The current embezzlement statute does not list them today. The Act remedies this by supplementing the embezzlement statute property list to include: (1) computers and computer networks; (2) financial instruments, computer data, programs and software, whether tangible or intangible, in a format readable by computers, in transit between computers or within a computer network, or located on paper or in any device; and (3) computer services.

Computer as instrument of forgery.⁴⁷ Forgery is normally thought of as the creation, alteration or deletion of a tangible writing (or thing) and the forgery statutes in Virginia are drafted in this manner.⁴⁸ Of course, computer data can be forged and the “forgery” of computer data does not involve something tangible in that sense. To address this, the Act provides that the creation, alteration, or deletion of any computer data, which if done on a tangible document would constitute a forgery, is also a forgery. That fact that such a forgery is not done on a tangible writing is no defense.

Encryption used in criminal activity.⁴⁹ Encryption software is readily available even to retail consumers and it is inexpensive. While lawyers may not use such software regularly, its use is

⁴⁴ Va. Code Ann. Section 18.2-152.8.

⁴⁵ Va. Code Ann. Section 18.2-111.

⁴⁶ 217 Va. 688, 232 S.E.2d 745 (1977).

⁴⁷ Va. Code Ann. Section 18.2-152.14.

⁴⁸ Va. Code Ann. Section 18.2-168 *et seq.*

⁴⁹ Va. Code Ann. Section 18.2-152.15.

ubiquitous in other endeavors. The Act defines encryption to mean the enciphering of intelligible data into unintelligible form or the deciphering of unintelligible data into intelligible form. The Act provides that if encryption is used to further a criminal activity, it is a separate and distinct offence from the predicate criminal activity and punishable as a Class 1 misdemeanor.

III. Other Provisions of the Act

Statute of Limitations. A civil action for injury resulting from a violation of the Act must be commenced before the earlier of five years from the last act in the course of conduct constituting the violation of the Act or two years after plaintiff discovers or reasonably should have discovered such last act in the course of conduct.⁵⁰ Prosecution of a crime under the Act must be commenced before the earlier of five years from the last act in a course of conduct or one year after the existence of the illegal act and identity of the offender are discovered by the Commonwealth, owner, or anyone else who is damaged.⁵¹

Personal Jurisdiction. In cases alleging injury arising from the transmission of UBE cases, personal jurisdiction may be exercised pursuant to Virginia's long arm statute.⁵² See the cases cited in Section II on the transmission of UBE.

Venue. For the purposes of determining proper venue under the Act, any alleged violation of the Act is to be considered to have been committed in any county or city in which: any act was performed in furtherance of any course of conduct which violated the Act; the owner has principal place of business in the Commonwealth; any offender had control of proceeds of the violation or of any books, records, documents, property, financial instrument, software, program, data, or other material or objects used in the furtherance of the violation; from which, to which or through which any access to a computer or computer network was made whether by wires, electromagnetic waves, microwaves, or any other means of communication; the offender resides; or in which any computer which is the object or an instrument of the violation is located at the

⁵⁰ Va. Code Ann. Section 18.2-152.12.F; 8.01-40.1.

⁵¹ Va. Code Ann. Section 18.2-152.9.

⁵² Va. Code Ann. Section 18.2-152.12.F; 8.01-328.1.

time of the offense.⁵³ Of particular significance to cases involving the transmission of UBE, the Act specifically provides that proper venue may be the county or city which is the location of any computer or computer network from which, to which or through which access is made. AOL, an Internet service provider, and Verizon Online Services, Inc., another online service provider, have several servers in Virginia.

Protection of secrecy, trade secrets and privacy during proceeding. Litigation under the Act may frequently involve the trade secrets of one or more parties to the litigation. Of course, such trade secrets may be of great value. Accordingly, a party possessing such trade secrets may need to protect such trade secrets from disclosure during the litigation. Bring an action under the Act may also put in the public record a set of pleadings or other documents which may unintentionally constitute a set of instructions that another person may use to do the same or similar act which is the subject of the complaint of the plaintiff. Further, such litigation could result in an invasion of the privacy of nonparties who complain about violations of the Act. The Act specifically addresses these issues. At a request of any party to the action, the court may, in its discretion, conduct all legal proceedings in such a way as to: (1) protect the secrecy and security of the computer, computer network, data, program and software; (2) trade secrets; and (3) privacy of non-parties who complain about violations.⁵⁴

III. Conclusion

The Virginia Computer Crimes Act appears to be a currently adequate and suitable legislative response to an evolving societal need to provide a civil remedy for violations of specific acts related to computers, computer networks, email, the Internet and related matters. Of course, such technologies are constantly changing and the Act will likely be in need of updating from time to time to meet these changes. In fact, as recently as 2004, the Virginia State Crime Commission was directed to examine the Computer Crimes Act and present its recommendations for modifications to the General Assembly. As a result, the current Act discussed herein is the product of these recent revisions to streamline the definitions, and clarify the scope of the Act to

⁵³ Va. Code Ann. Section 18.2-152.10.

⁵⁴ Va. Code Ann. Section 18.2-152.12.D.

promote further enforcement. Unfortunately, the Act still appears to be under utilized by business law practitioners. While the Act was enacted in 1983 and became effective in 1984, there is little published case law under the Act. Perhaps this is the case because the Act is a criminal statute and embodied in Virginia Code Title 18.2, “Crimes and Offenses Generally,” a location not well known to Virginia business lawyers. It may be that this location is inappropriate for a civil cause of action related to computers and it may be less appropriate in the future as the need for the application of such remedies increases. However, whatever the location, the Act may be very favorable for plaintiff’s counsel. It has very favorable provisions on personal jurisdiction and venue and it authorizes attractive civil remedies, including treble damages and attorneys’ fees.