GMU 9th Annual Ethics Update

# The Ethics of Electronic Discovery and Identity Theft

(Time)

1. Electronic Discovery (E-Discovery)
    a. Overview (3)
    b. Attorney must have technical competence. (6)
        i. Rule 1.1: Competence
        ii. Fed. R. Civ. P. 26(a)(1)(B), 26(b)(2)(B), Fed. R. Civ. P. 26(f)
        iii. Virginia Supreme Court Rules 4:1(a) and 4:9(a)
    c. Ethical obligations to court and opposing counsel (6)
        i. Rule 3.3: Candor Toward The Tribunal.
        ii. Rule 3.4: Fairness To Opposing Party And Counsel.
    d. Inadvertent disclosure of privileged information (5)
        i. Rule 4.4: Respect for Rights of Third Persons.
        ii. Fed. R. Civ. P. 26(f), Fed. R. Civ. P. 16(b), and Fed. R. Civ. P. 25(b)(5)(B).
    e. Ethical issues related to meta-data (7)
2. E-Discovery Case Study: Virginia Computer Crimes Act (VCCA), Va. Code §18.2-152.1 et seq.
    a. Overview of VCCA (10)
        i. Commonwealth v. Jaynes series of cases
    b. E-Discovery in a civil suit for damages arising under the VCCA (5)
3. Identity Theft Prevention in Virginia
    a. Rule 1.6: Confidentiality of Information (2)
    b. Va. Code §18.2-186.6: Breach of personal information notification. (6)
        i. "Entity" includes "*any [] legal entity*"
        ii. "Personal Information" consists of first name or first initial and last name and (a) SSN; (b) Driver's License Number; (c) Financial account information and PIN or password; unless redacted or encrypted.
        iii. Duty to notify VA Office of Attorney General and all affected parties.

Appendices:

A. Virginia Computer Crimes Act, Va. Code §18.2-152.1 et seq.
B. Breach of personal identification notification, Va. Code §18.2-186.6.

GMU 9th Annual Ethics Update

# The Ethics of Electronic Discovery and Identity Theft

## 1. Electronic Discovery (E-Discovery)[1]

a. Overview

i. What is E-Discovery?
Electronic discovery encompasses discovery of electronic data which could be recovered from computers, PDAs, memory cards, cellular telephones, networking equipment and other devices that store and process electronic data.

ii. As technology advances, litigators must keep pace in order to provide the best possible representation to their clients and meet their ethical obligations.

iii. Sources for the lawyer's duty include:
1. State Professional Conduct Rules.
2. Federal Rules of Civil Procedure, Section V, Discovery and Depositions.
3. Local court rules.
4. State ethics opinions.

b. Attorney must have technical competence.
Attorneys must have an understanding of the rules of discovery and of the IT systems of their clients and their client's opponent in order to provide competent representation.

i. Rule 1.1: Competence: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

ii. Federal Rules of Civil Procedure
Lawyers must have sufficient technical understanding to provide accurate descriptions and definitions of electronically stored information, to understand the costs of production of various kinds of electronic data.

1. Fed. R. Civ. P. 26(a)(1)(A)(ii) requires that the initial disclosure to opposing counsel contain "a copy — or a description by category and location — of all documents, *electronically stored information*, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses,

[1] Adapted from the American Bar Association's "Ethical Issues in E-Discovery" materials, June 4, 2008.

unless the use would be solely for impeachment;" (emphasis added)

2. Fed. R. Civ. P. 26(b)(2)(B) creates an exception for the production of data that would create an unreasonable burden on the opposing party: "A party need not provide discovery of *electronically stored information* from sources that the party identifies as not reasonably accessible because of undue burden or cost." (emphasis added)

3. Fed. R. Civ. P. 26(f)(3)(C) provides that " any issues about disclosure or discovery of *electronically stored information*, including the form or forms in which it should be produced" (emphasis added) may be discussed at the Rule 26(f) discovery planning conference.

iii. Virginia has not adopted any specific rules governing discovery of electronically stored information. Any such discovery would be included in the "request for production of documents or things" (Virginia Supreme Court Rule 4:1(a)), which provides for production of " any designated documents (including … other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form)" (Virginia Supreme Court Rule 4:9(a)).

Attorneys must understand different forms of electronically stored information and how and where it is stored in their client's systems and their client's opponent's systems. This requires an understanding of operating systems, various devices (computers, PDAs, network equipment) and the life cycle of data as it is initially generated, possibly transmitted, backed up or archived, and removed or deleted.[2]

Furthermore, attorneys must understand the various data types and how those data types could be produced and "translated, if necessary, … into a reasonably usable form." (Virginia Supreme Court Rule 4:9(a)). Metadata may provide the key to the foundation of a case, but if production of the metadata in a native format is "unduly burdensome" then the court may order metadata to be produced in a translated format.[3]

c. <u>Ethical obligations to court and opposing counsel</u>
Lawyers owe a duty to the court to ensure that the data provided by their client is complete and accurate. To fulfill this obligation, the lawyer must

---

[2] *See* The Committee Note to Rule 26(f) which states that it may be "important for counsel to become familiar with [its client's information] systems before the [discovery-planning] conference."
*See also Zubulake v. UBS Warburg*, 229 F.R.D. 422, 432 (S.D.N.Y. 2004), which states "[C]ounsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture."

[3] *See Michigan First Credit Union v. Cumis Ins. Soc.*, 2007 U.S. Dist. LEXIS 84842 (E.D. Mich. November 16, 2007) where the court rejected a request to produce metadata in a "'native format'" but said that the PDF copy of the data contained the relevant metadata in an alternate format.

sufficiently supervise the discovery process and possess the technical competence to understand that the client is in compliance.

i. Rule 3.3: Candor Toward The Tribunal.
"(a) A lawyer shall not knowingly: (1) make a false statement of fact or law to a tribunal; (2) fail to disclose a fact to a tribunal when disclosure is necessary to avoid assisting a criminal or fraudulent act by the client, subject to Rule 1.6; … (4) offer evidence that the lawyer knows to be false. If a lawyer has offered material evidence and comes to know of its falsity, the lawyer shall take reasonable remedial measures."

Lawyers have a duty to the opposing party and counsel that requires that a lawyer must not destroy evidence or obstruct the discovery of relevant evidence, and the lawyer must supervise the discovery process to ensure that her client is complying with this duty. Failure to do so could result in sanctions[4].

ii. Rule 3.4: Fairness To Opposing Party And Counsel.
"A lawyer shall not:
"(a) Obstruct another party's access to evidence or alter, destroy or conceal a document or other material having potential evidentiary value for the purpose of obstructing a party's access to evidence. A lawyer shall not counsel or assist another person to do any such act. …
"(e) Make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by

---

[4] *See:*

- *Qualcomm Inc. v. Broadcom Corp.*, No. 05-CV-1958-B(BLM) (S.D. Cal. Aug. 13, 2007) (Order to Show Cause Why Sanctions Should Not Be Imposed)
- *Qualcomm v. Broadcom, 2008 WL 638108* (S.D Cal. Mar. 5, 2008) remanded the issue of sanctions against the Qualcomm attorneys and held the attorney-client privilege was waived under the self-defense exception.
- On May 5, 2008, Qualcomm filed a notice of appeal of the March 5, 2008 "Order Remanding in Part Order of Magistrate Court re Motion for Sanctions Dated 1/07/08" ("Remand Order").
- On May 19, 2008, attorneys Batchelder, Mammen, Leung and Patch filed notices of cross appeal. Doc. Nos. 797, 798.
- On its own motion, the S.D Cal. issued an order on May 29, 2008, vacating all pending hearing dates because the S.D Cal. concluded that, as a result of the appeal and cross appeals, jurisdiction has been transferred from the S.D Cal. to the United States Court of Appeals for the Federal Circuit. Doc. No. 812.
- On July 7, 2008 Magistrate Judge in S. D. Cal. denies Broadcom's Motion for Reconsideration, stating that jurisdiction is now in the Fed. Circuit.
- Fed. Circuit issued a decision on the patent claims in the case, but did not rule on the sanctions order yet in Broadcom Corporation v. Qualcomm Incorporated, No. 2008-1199 (Fed. Cir. 9/24/2008) (Fed. Cir., 2008).

an opposing party."

d. Inadvertent disclosure of privileged information
In electronic discovery, the probability of turning over privileged information to the opposing party is increased due to the sheer volume of information disclosed, the use of search terms to locate materials subject to discovery and the possibility of producing metadata with privileged content that accompanies non-privileged data.

Attorneys can proactively protect against this by using a number of techniques including: placing a conspicuous label on each page of a document or in the subject or other header of an electronic mail message that the document contains privileged information; using encryption for files and communications, including electronic mail messages, that are subject to privilege; converting documents to a read-only format and eliminating metadata before sending to third parties, such as converting a document to a PDF format.

If attorneys get in the habit of making these clear identifications in advance of litigation, then weeding out privileged information can be accomplished more easily using automated tools.

The Virginia rule provides some protection to attorneys when inadvertent disclosure occurs, but the ABA model rules adopted by many states and the Federal Rules of Civil Procedure offer varying levels of protection.

i. Rule 4.4: Respect for Rights of Third Persons.
Virginia did not adopt the ABA Model Rule 4.4(b) which requires only a notification to the disclosing party that privileged information was received. Rather, Virginia requires that the recipient "return unread" the privileged information to the disclosing party. *See Virginia Legal Ethics Opinions 1702 and 1786.*

ii. Fed. R. Civ. P. 26(f) requires the parties to confer on claims of privilege or work product.

Fed. R. Civ. P. 16(b) allows courts to include "any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production" in their scheduling orders.

Fed. R. Civ. P. 25(b)(5)(B) provides a "clawback" provision, requiring the receiving party to sequester the privileged information, but with no requirement of notification or return of the privileged information to the disclosing party. Furthermore,

the court can decide if the documents are privileged or if the privilege was waived, and can then allow the receiving party to use the information. The Federal Rules do not provide a rule for determination of when the privilege is waived by production.

e. Ethical issues related to meta-data

Metadata consists of data which is not generally visible when data is viewed, but which is stored in the electronic representation of the data. Metadata includes additional information used by the application(s) that interact with the electronic representation of the data, such as: time and date stamps, revision history, track changes in the case of documents; header and routing information in the case of electronic mail messages; indices and other structures that aid the application(s) in displaying and managing the electronic data in the case of most file types.

Because metadata is not generally visible when an electronic file is displayed or printed, it is often overlooked. However, metadata can contain privileged or confidential data in cases where the public display of the data is not privileged. For example, a document file may contain metadata with information on the persons who edited it, and what their revisions included, which could be used to show a conspiracy, while the final version of the document itself provides no clues as to how the document was created. Likewise, the date or time stamp in an electronic mail message or a document can be crucial in demonstrating a sequence of events, whereas the final version may not betray its history.

At this point it is unclear as to whether privilege related to metadata is waived upon production of the overall data file, and attorneys must look to local ethics rules and opinions based upon the venue and jurisdiction of the litigation. Virginia has yet to opine on metadata. Maryland State Bar Association, Committee on Ethics, Opinion 2007-09 (November 2006) allows an attorney to "review[] or make[] use of the metadata without first ascertaining whether the sender intended to include such metadata." District of Columbia Bar Legal Ethics Committee Opinion 341 (September 2007) allows review of the metadata unless the receiving attorney knows that it was sent inadvertently, and also cautions review of the applicable Federal Rules of Civil Procedure.

As discussed *supra*, the Federal Rules require that the production or non-production of metadata be part of the discovery plan, and that issues related to privilege that arise during discovery be resolved by the parties or by an order of the court.

2. E-Discovery Case Study: Virginia Computer Crimes Act (VCCA), Va. Code §18.2-152.1 et seq.

a. Overview of VCCA

Virginia Code §8.01-328.1, which covers personal jurisdiction, was amended to include a specific reference to the Virginia Computer Crimes Act: "B. Using a computer or computer network located in the Commonwealth shall constitute an act in the Commonwealth. For the purposes of this subsection, "use" and "computer network" shall have the same meanings as those contained in § 18.2-152.2.

The VCCA penalizes the "Transmission of unsolicited bulk electronic mail" in §18.2-152.3:1 and penalizes "Computer trespass" in §18.2-152.4, and then provides a civil cause of action for damages caused by the criminal acts in §18.2-152.12. The civil relief allows for statutory damages of $25,000 per day or $1 per email, whichever is greater, for an Email Service Provider (EMSP) who is harmed by the "unsolicited bulk electronic mail." Any party harmed by a "computer trespass" must show actual damages.

The criminal provisions for the "Transmission of unsolicited bulk electronic mail" have been ruled unconstitutional by the Supreme Court of Virginia (*see Jaynes v. Commonwealth, Record No. 062388 (Va. 9/12/2008) (Va., 2008), infra)*, and therefore the civil damages which rely upon a violation of the criminal provisions are now unavailable to civil litigants. However, the Supreme Court of Virginia distinguished the criminal matter in Jaynes from a computer trespass case in a civil setting, so a civil action for violation of the "Computer trespass" provisions is still available.

i. Commonwealth v. Jaynes series of cases
    1. 2003: Jaynes sends tens of thousands of emails to AOL's servers in Virginia from his home in North Carolina.
    2. Commonwealth v. Jaynes, Loudoun County, Virginia Circuit Court, April 8, 2005
        a. A jury convicted Jaynes of three counts of violating Code § 18.2-152.3:1, and the circuit court sentenced Jaynes to three years in prison on each count, with the sentences to run consecutively for an active term of imprisonment of nine years.
    3. Jaynes v. Commonwealth, 48 Va. App. 673, 634 S.E.2d 357 (2006).
        a. CAV affirms the conviction, holding "that the trial court had jurisdiction over this case and that Code § 18.2-152.3:1 does not violate the First Amendment, does not violate the Dormant Commerce Clause, and is not unconstitutionally vague, appellant's convictions are affirmed."

4. Jaynes v. Com., 657 S.E.2d 478, 275 Va. 341 (Va., 2008)
    a. SCV holds: "that the circuit court had jurisdiction over Jaynes. We also hold that Jaynes does not have standing to make a First Amendment overbreadth challenge to Code § 18.2-152.3:1. Finally, we hold that Jaynes' vagueness argument is without merit, and the statute does not violate the Commerce Clause. We will therefore affirm the judgment of the Court of Appeals upholding these convictions and sentences."
5. Jaynes v. Commonwealth, Record No. 062388 (Va. 9/12/2008) (Va., 2008)
    a. Rehearing on constitutionality of the VCCA anti-SPAM provisions, upon rehearing pursuant to orders dated April 28, 2008 and May 19, 2008.
    b. SCV holds that it does have jurisdiction over Jaynes, even though Jaynes was located in North Carolina.
    c. SCV holds that the VCCA anti-SPAM provisions do not amount to trespass statute when used in the criminal context.
    d. SCV holds that the VCCA is "unconstitutionally overbroad on its face because it prohibits the anonymous transmission of all unsolicited bulk e-mails including those containing political, religious or other speech protected by the First Amendment to the United States Constitution" in the anti-SPAM criminal context.
    e. SCV reverses Jaynes' conviction.

b. E-Discovery in a civil suit for damages arising under the VCCA
    i. In the anti-SPAM context, the VCCA required forged or falsified header or routing information. Thus, a civil litigant would have to ensure that its systems were set up to collect and store this metadata, header and routing information, and be able to produce this information in a discovery request.

    ii. In the criminal trespass context, a civil litigant would need to preserve and be able to produce metadata such as network router, server and computer logs to substantiate the trespass action. Furthermore, a civil litigant would need to understand how the trespass was committed, what systems were used by the intruder, and what discovery requests to make for information, including metadata, from the intruder's systems.

3. Identity Theft Prevention in Virginia

   The Virginia legislature has passed a new law entitled "Breach of personal information notification" which requires entities to notify individuals when the individual's "personal information" when the entity has a "breach of the security of [the entity's] system."

   This law could apply to law firms if they hold client information and suffer a data breach. Additionally, you may need to advise your client in the event of a data breach, and you further may want to pursue a computer trespass action under the VCCA, *supra*, to recover the costs of remedying the breach, including the required notification under this statute.

   Entities are protected if they keep "personal information" in an encrypted or redacted form, and can save the embarrassment of a public notification in the event of a data breach if they use encryption or redact the data.

   a. Rule 1.6: Confidentiality of Information
      "(a) A lawyer shall not reveal information protected by the attorney-client privilege under applicable law or other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client … "

   b. Va. Code §18.2-186.6: Breach of personal information notification.
      i. "Entity" includes "*any [] legal entity*"
      ii. "Personal Information" consists of first name or first initial and last name and (a) SSN; (b) Driver's License Number; (c) Financial account information and PIN or password; unless redacted or encrypted.
      iii. Duty to notify VA Office of Attorney General and all affected parties.

# APPENDIX A

**VIRGINIA CODE**
**TITLE 8.01. CIVIL REMEDIES AND PROCEDURE**
**CHAPTER 9. PERSONAL JURISDICTION IN CERTAIN ACTIONS**
**SECTION 8.01-328.1 (2003)**

**§ 8.01-328.1. When personal jurisdiction over person may be exercised.**

A. A court may exercise personal jurisdiction over a person, who acts directly or by an agent, as to a cause of action arising from the person's:

1. Transacting any business in this Commonwealth;
2. Contracting to supply services or things in this Commonwealth;
3. Causing tortious injury by an act or omission in this Commonwealth;
4. Causing tortious injury in this Commonwealth by an act or omission outside this Commonwealth if he regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in this Commonwealth;
5. Causing injury in this Commonwealth to any person by breach of warranty expressly or impliedly made in the sale of goods outside this Commonwealth when he might reasonably have expected such person to use, consume, or be affected by the goods in this Commonwealth, provided that he also regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered in this Commonwealth;
6. Having an interest in, using, or possessing real property in this Commonwealth;
7. Contracting to insure any person, property, or risk located within this Commonwealth at the time of contracting;
8. Having (i) executed an agreement in this Commonwealth which obligates the person to pay spousal support or child support to a domiciliary of this Commonwealth, or to a person who has satisfied the residency requirements in suits for annulments or divorce for members of the armed forces pursuant to § 20-97 provided proof of service of process on a nonresident party is made by a law-enforcement officer or other person authorized to serve process in the jurisdiction where the nonresident party is located, (ii) been ordered to pay spousal support or child support pursuant to an order entered by any court of competent jurisdiction in this Commonwealth having in personam jurisdiction over such person, or (iii) shown by personal conduct in this Commonwealth, as alleged by affidavit, that the person conceived or fathered a child in this Commonwealth;
9. Having maintained within this Commonwealth a matrimonial domicile at the time of separation of the parties upon which grounds for divorce or separate maintenance is based, or at the time a cause of action arose for divorce or separate maintenance or at the time of commencement of such suit, if the other party to the matrimonial relationship resides herein; or
10. Having incurred a tangible personal property tax liability to any political subdivision of the Commonwealth.

Jurisdiction in subdivision 9 is valid only upon proof of service of process pursuant to § 8.01-296 on the nonresident party by a person authorized under the provisions of § 8.01-320. Jurisdiction under subdivision 8 (iii) of this subsection is valid only upon proof of personal service on a nonresident pursuant to § 8.01-320.

B. Using a computer or computer network located in the Commonwealth shall constitute an act in the Commonwealth. For purposes of this subsection, "use" and "computer network" shall have the same meanings as those contained in § 18.2-152.2.

C. When jurisdiction over a person is based solely upon this section, only a cause of action arising from acts enumerated in this section may be asserted against him; however, nothing contained in this chapter shall limit, restrict or otherwise affect the jurisdiction of any court of this Commonwealth over foreign corporations which are subject to service of process pursuant to the provisions of any other statute.

**VIRGINIA CODE**
**TITLE 18.2. CRIMES AND OFFENSES GENERALLY**
**CHAPTER 5. CRIMES AGAINST PROPERTY**
**ARTICLE 7.1. COMPUTER CRIMES**
**SECTIONS 18.2-152.2, 152.3:1, 152.4, 152.12 (2003)**
**(including amendments by Acts 2003, ch. 987 & 1016, approved April 3, 2003)**

**§ 18.2-152.2. Definitions.**

For purposes of this article:

"Computer" means an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. The term "computer" includes any connected or directly related device, equipment, or facility which enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.

"Computer data" means any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. "Computer data" may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.

"Computer network" means two or more computers connected by a network.

"Computer operation" means arithmetic, logical, monitoring, storage or retrieval functions and any combination thereof, and includes, but is not limited to, communication with, storage of data to, or retrieval of data from any device or human hand manipulation of electronic or magnetic impulses. A "computer operation" for a particular computer may also be any function for which that computer was generally designed.

"Computer program" means an ordered set of data representing coded instructions or statements that, when executed by a computer, causes the computer to perform one or more computer operations.

"Computer services" means computer time or services, including data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

"Computer software" means a set of computer programs, procedures and associated documentation concerned with computer data or with the operation of a computer, computer program, or computer network.

"Electronic mail service provider" means any person who (i) is an intermediary in sending or receiving electronic mail and (ii) provides to end-users of electronic mail services the ability to send or receive electronic mail.

"Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computerized representation thereof.

"Network" means any combination of digital transmission facilities and packet switches, routers, and similar equipment interconnected to enable the exchange of computer data.

"Owner" means an owner or lessee of a computer or a computer network or an owner, lessee, or licensee of computer data, computer programs, or computer software.

"Person" shall include any individual, partnership, association, corporation or joint venture.

"Property" shall include:

1. Real property;
2. Computers and computer networks;
3. Financial instruments, computer data, computer programs, computer software and all other personal property regardless of whether they are:
a. Tangible or intangible;
b. In a format readable by humans or by a computer;
c. In transit between computers or within a computer network or between any devices which comprise a computer; or
d. Located on any paper or in any device on which it is stored by a computer or by a human; and
4. Computer services.

A person "uses" a computer or computer network when he attempts to cause or causes:

1. A computer or computer network to perform or to stop performing computer operations;
2. The withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or
3. A person to put false information into a computer.

A person is "without authority" when he has no right or permission of the owner to use a computer or he uses a computer or computer network in a manner exceeding such right or permission.

**§ 18.2-152.3:1. Transmission of unsolicited bulk electronic mail; penalty.**

A. 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 unsolicited bulk electronic mail 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) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic mail transmission information or other routing information; (ii) has only limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (iii) is marketed by that person acting alone or with another for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information is guilty of a Class 1 misdemeanor.

B. A person is guilty of a Class 6 felony if he commits a violation of subsection A and:

1. The volume of UBE transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period; or

2. The revenue generated from a specific UBE transmission exceeded $1,000 or the total revenue generated from all UBE transmitted to any EMSP exceeded $50,000.

C. A person is guilty of a Class 6 felony if he knowingly hires, employs, uses, or permits any minor to assist in the transmission of UBE in violation of subdivision B 1 or subdivision B 2.

**§ 18.2-152.4. Computer trespass; penalty.**

A. It shall be unlawful for any person to use a computer or computer network without authority and with the intent to:

1. Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network;

2. Cause a computer to malfunction, regardless of how long the malfunction persists;

3. Alter or erase any computer data, computer programs, or computer software;

4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;

5. Cause physical injury to the property of another;

6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

B. Any person who violates this section shall be guilty of computer trespass, which offense shall be punishable as a Class 1 misdemeanor. If there is damage to the property of another valued at $2,500 or more caused by such person's malicious act in violation of this section, the offense shall be punishable as a Class 6 felony.

C. Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to computers, computer data, computer networks, computer operations, computer programs, computer services, or computer software or to create any liability by reason of terms or conditions adopted by, or technical measures implemented by, a Virginia-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this article. Nothing in this section shall be construed to prohibit the monitoring of computer usage of, the otherwise lawful copying of data of, or the denial of computer or Internet access to a minor by a parent or legal guardian of the minor.

**§ 18.2-152.12. Civil relief; damages.**

A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained, and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

B. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, the injured person, other than an electronic mail service provider, may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the lesser of $10 for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or $25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

C. If the injury under this article arises from the transmission of unsolicited bulk electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider where the defendant has knowledge of the authority or policies of the EMSP or where the authority or policies of the EMSP are available on the electronic mail service provider's website, an injured electronic mail service provider may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover $1 for each and every intended recipient of an unsolicited bulk electronic mail message where the intended recipient is an end user of the EMSP or $25,000 for each day an attempt is made to transmit an unsolicited bulk electronic mail message to an end user of the EMSP. In calculating the statutory damages under this provision, the court may adjust the amount awarded as necessary, but in doing so shall take into account the number of complaints to the EMSP generated by the defendant's messages, the defendant's degree of culpability, the defendant's prior history of such conduct, and the extent of economic gain resulting from the conduct. Transmission of electronic mail from an organization to its members shall not be deemed to be unsolicited bulk electronic mail.

D. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party and in such a way as to protect the privacy of nonparties who complain about violations of this section.

E. The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

F. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1. In actions alleging injury arising from the transmission of unsolicited bulk electronic mail, personal jurisdiction may be exercised pursuant to § 8.01-328.1.

# APPENDIX B

**VIRGINIA CODE**
**TITLE 18.2. CRIMES AND OFFENSES GENERALLY**
**CHAPTER 6. CRIMES INVOLVING FRAUD**

§ 18.2-186.6. Breach of personal information notification.

A. As used in this section:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

"Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

"Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

"Financial institution" has the meaning given that term in 15 U.S.C. § 6809(3).

"Individual" means a natural person.

"Notice" means:

1. Written notice to the last known postal address in the records of the individual or entity;

2. Telephone notice;

3. Electronic notice; or

4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Substitute notice consists of all of the following:

a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

c. Notice to major statewide media.

Notice required by this section shall not be considered a debt communication as defined by the Fair Debt Collection Practices Act in 15 U.S.C. § 1692a.

Notice required by this section shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the individual or entity to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; and

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data

elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

1. Social security number;

2. Driver's license number or state identification card number issued in lieu of a driver's license number; or

3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

1. Five digits of a social security number; or

2. The last four digits of a driver's license number, state identification card number, or account number.

B. If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

C. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the

individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

D. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.

E. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681(a)(p), of the timing, distribution, and content of the notice.

F. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of the security of the system.

G. An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section.

H. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section.

I. Except as provided by subsections J and K, pursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action to address violations of this section. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.

J. A violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator.

K. A violation of this section by an individual or entity regulated by the State Corporation Commission's Bureau of Insurance shall be enforced exclusively by the State Corporation Commission.

L. The provisions of this section shall not apply to criminal intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the Commonwealth and the organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ 52-12 et seq.) of Title 52.