Senate Counsel, Research, and Fiscal Analysis

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate
State of Minnesota

S.F. No. 927 - False and Deceptive Commercial E-mail

Author: Senator Dan Sparks

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890) MG

Date: March 11, 2005

The bill adds to Minnesota's consumer protection laws by prohibiting the transmission of false, misleading, or deceptive commercial electronic mail to or from a computer in Minnesota, while making provisions to exclude transactional messages as part of an established commercial relationship. The bill also prohibits unauthorized access of a computer for the purpose of initiating transmission of electronic mail messages. The bill provides criminal penalties, ranging from misdemeanor to felony depending upon the extent of the activity and prior convictions, for both the transmission of false, misleading, or deceptive electronic mail and unauthorized access of a computer. The bill provides for civil actions, granting the Attorney General standing to initiate civil action, and establishes statutory limits on damages.

MSG:cs

I. Introduction

Mr. Chairman and members of the Committee, thank you for the opportunity to testify today on behalf of America Online in support of HF 1318. SF 927

ISPs are on the front lines of the fight against spam. Over half the traffic on the Internet today is spam. Sophisticated spammers send millions of e-mail messages quickly, at an extremely low cost, with no repercussions. The sheer volume of spam, which is growing at an exponential rate, is overwhelming existing network systems, as well as consumers' in-boxes. Spam burdens the capacity of ISP networks, requiring them to build additional capacity, and is the most significant consumer concern about the Internet today. Spam fighting is thus a major priority for all ISPs. They devote millions of dollars and round-the-clock teams of technical experts to block on a daily basis billions of spam messages from reaching customers, to sue spammers (AOL alone has sued over 100 spammers), and to work actively to assist law enforcement in bringing enforcement actions. Unfortunately, civil enforcement by the Federal Trade Commission and by ISPs has not deterred "king-pin" spammers from earning significant profits while living in the U.S. sending millions of spam messages daily. Their messages are unfortunately all too familiar to the members of this Committee. Rarely a minute passes without American consumers and their children being bombarded with e-mail messages promoting pornographic web sites, illegal pirated software, illegal prescription drugs, "get rich quick" scams, and the like.

And there are other prominent and equally important costs of spam. It may introduce viruses, worms, and Trojan horses into personal and business computer systems, including those that support our national infrastructure. Spam also offers fertile ground for deceptive trade

practices. The Federal Trade Commission estimates that nearly 66 percent of spam contains some kind of deception, either in the content, the "subject" line, or the "from" line. And an astonishing 90 percent of spam involving investment and business opportunities contains indicia of false claims. This rampant deception has the potential to undermine Americans' trust of valid information on the Internet and threaten the future viability of all e-commerce.

Our company has concluded that measures holding the greatest promise in the difficult battle against spam are technology solutions coupled with criminal penalties aimed at "outlaw spammers" who rely on falsification and hacking techniques to frustrate the technologies that ISPs and consumers use to fight spam. For this reason AOL strongly supports HF 1318 and similar state laws introduced in Iowa, New Jersey, and Missouri that criminalize use of the leading falsification and hacking techniques that are used by sophisticated "outlaw spammers." They also strongly supported the criminal prohibitions against outlaw spam in the federal CAN-SPAM Act, on which HF 1318 is modeled. Effective federal and state enforcement against spammers based in the U.S., who account for most of the offensive material received in e-mail boxes every day, would deter other spammers so that they find a different line of work, and thereby reduce the volume of spam.

II. HF 1318 Addresses the Ways in Which Spammers Penetrate User Inboxes

The purpose of HF 1318 is to criminalize the sending of bulk commercial e-mail (commonly known as "spam") through fraudulent and deceptive means. The bill would amend Minnesota's criminal law to prohibit five principal techniques that spammers use to evade ISP and end user filtering software and hide their trails. Penalties for violations of these new

criminal prohibitions would include imprisonment, fines, and forfeiture of proceeds. Offenders may also be subject to civil enforcement actions brought by the Attorney General.

1. Prohibiting All Major Current Spammer Falsification Tactics

HF 1318 prohibits the five principal deceptive techniques that spammers currently use to evade filtering software and get bulk unwanted e-mails into inboxes.

First, the bill prohibits knowingly and materially falsifying the header information, and initiating bulk commercial e-mail accompanied by or containing that false header information. More specifically, the bill prohibits forging information regarding the origin of an e-mail message, the route of the message, the destination of the message, or information authenticating the user for network security or network management purposes—for example, as a "trusted sender" who abides by appropriate consumer protection rules. This last type of forgery will be particularly important in the future, as ISPs and legitimate marketers develop more secure e-mail systems that use authentication methods to filter out spam by bad actors. However, these systems would be useless if outlaw spammers are allowed to counterfeit the authentication mechanisms upon which such systems will depend.

Second, the bill prohibits knowingly registering for five or more e-mail accounts or user names or two or more Internet domain names using information that materially falsifies the identity of the actual registrant, and intentionally initiating bulk commercial e-mail from those accounts or domains. This provision targets deceptive "account churning," a common outlaw spammer technique that works as follows: The spammer registers (usually by means of an automatic computer program, or by means of individuals located in other countries) for large numbers of e-mail accounts or domain names, using false registration information, then sends

bulk spam from one account or domain after another. This technique stays ahead of ISP filters by hiding the source, size, and scope of the sender's mailings, and prevents the e-mail account provider or domain name registrar from identifying the registrant as a spammer and denying his registration request. Falsifying registration information for domain names also violates a basic contractual requirement for domain name registrations.

Third, the bill prohibits knowingly and falsely asserting the right to use five or more Internet Protocol ("IP") addresses and intentionally initiating the transmission of bulk commercial e-mail from those addresses. This provision addresses another significant hacker spammer technique for hiding identity that is a common and pernicious alternative to domain name registration—hijacking unused Internet Protocol ("IP") addresses and using them as launch pads for spam. Hijacking large blocks of IP address space is not difficult: Spammers simply falsely assert that they have the right to use that space, and obtain an Internet connection for the addresses. Hiding behind those addresses, they can then send vast amounts of spam that is extremely difficult to trace.

Fourth, the bill prohibits knowingly hacking into another person's computer system and sending bulk spam from or through that system. This would criminalize the common spammer technique of obtaining access to other people's e-mail accounts on an ISP's e-mail network, for example by password theft or by inserting a "Trojan horse" program—that is, a program that unsuspecting users download onto their computers and that then takes control of those computers—to send bulk spam.

Fifth, the bill prohibits conspiring with others in a violation of these activities, a prohibition aimed at king pin spammers, who require or recruit others to engage in violations.

2. Graduated Penalties

Penalties for these violations range from a gross misdemeanor to a felony, based on culpability, and include monetary awards which the Attorney General and injured ISPs can collect (up to twenty five thousand dollars a day).

The bill also wisely includes penalty enhancements for offenders who obtained e-mail addresses through two improper means: first, harvesting e-mail addresses, a practice of automatic collection of e-mail addresses, which has made users who post their e-mail addresses on websites and chatrooms pay in an avalanche of spam; second, so-called "dictionary attacks" in which an attacker launches a brute force spam attack by randomly generating possible working e-mail addresses to a popular Internet domain (such as "aol.com"). This approach creates very heavy network load and returned messages.

In addition, it provides for forfeiture of spammer revenues and instrumentalities used in the offense, as well as A.G. civil enforcement of violations, which may prove useful in some instances.

III. HF 1318 Would Not Be Preempted and Is Constitutional

Although the federal CAN-SPAM law preempts most state e-mail regulation, it contains express exemptions from preemption for state laws that prohibit acts of falsification in commercial e-mail or computer crimes. The legislative history to this provision indicates that Congress intended specifically to preserve state criminal spam laws, like the Virginia spam law, that target falsification in connection with commercial e-mail. HF 1318 is precisely such a law.

Furthermore, HF 1318 would comply fully with the First Amendment to the U.S. Constitution. Rather than targeting speech, it instead targets e-mailing techniques used to steal

computer services and trespass on private computers and computer networks. Furthermore, to the extent that any First Amendment interest is implicated by this bill, it addresses only commercial speech and only commercial speech that is "misleading" by virtue of falsifying the source of the e-mail message. It, therefore, fails the first prong of the test set forth in *Central Hudson Gas & Electric Corp. v. Pub. Service Comm'n*, 447 U.S. 557, 566 (1980). Finally, HF 1318 addresses commercial, and not non-commercial, electronic mail messages, because, based upon the Committee's review of the spam problem, the overwhelming majority of predatory and abusive e-mail is commercial e-mail within the meaning of this bill, or is otherwise sent for private pecuniary gain.

IV. Conclusion

Mr. Chairman and members of the Committee, HF 1318 would provide an important new arsenal for Minnesota law enforcement to protect consumers in this state from spam. AOL and other Internet service providers strongly support this legislation and hope that it will be enacted this year. Thank you for considering our views.

2. Graduated Penalties

Penalties for these violations range from a gross misdemeanor to a felony, based on culpability, and include monetary awards which the Attorney General and injured ISPs can collect (up to twenty five thousand dollars a day).

The bill also wisely includes penalty enhancements for offenders who obtained e-mail addresses through two improper means: first, harvesting e-mail addresses, a practice of automatic collection of e-mail addresses, which has made users who post their e-mail addresses on websites and chatrooms pay in an avalanche of spam; second, so-called "dictionary attacks" in which an attacker launches a brute force spam attack by randomly generating possible working e-mail addresses to a popular Internet domain (such as "aol.com"). This approach creates very heavy network load and returned messages.

In addition, it provides for forfeiture of spammer revenues and instrumentalities used in the offense, as well as A.G. civil enforcement of violations, which may prove useful in some instances.

III. HF 1318 Would Not Be Preempted and Is Constitutional

Although the federal CAN-SPAM law preempts most state e-mail regulation, it contains express exemptions from preemption for state laws that prohibit acts of falsification in commercial e-mail or computer crimes. The legislative history to this provision indicates that Congress intended specifically to preserve state criminal spam laws, like the Virginia spam law, that target falsification in connection with commercial e-mail. HF 1318 is precisely such a law.

Furthermore, HF 1318 would comply fully with the First Amendment to the U.S. Constitution. Rather than targeting speech, it instead targets e-mailing techniques used to steal

computer services and trespass on private computers and computer networks. Furthermore, to the extent that any First Amendment interest is implicated by this bill, it addresses only commercial speech and only commercial speech that is "misleading" by virtue of falsifying the source of the e-mail message. It, therefore, fails the first prong of the test set forth in *Central Hudson Gas & Electric Corp. v. Pub. Service Comm'n*, 447 U.S. 557, 566 (1980). Finally, HF 1318 addresses commercial, and not non-commercial, electronic mail messages, because, based upon the Committee's review of the spam problem, the overwhelming majority of predatory and abusive e-mail is commercial e-mail within the meaning of this bill, or is otherwise sent for private pecuniary gain.

IV. Conclusion

Mr. Chairman and members of the Committee, HF 1318 would provide an important new arsenal for Minnesota law enforcement to protect consumers in this state from spam. AOL and other Internet service providers strongly support this legislation and hope that it will be enacted this year. Thank you for considering our views.

Senate Counsel, Research, and Fiscal Analysis

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 1225 - Broadband Revolving Loan Fund

Author: Senator Steve Kelley

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890) MSG

Date: March 11, 2005

The bill creates the broadband revolving loan fund under the auspices of the Minnesota Public Facilities Authority for the express purposes of making loans to governmental units for local communications infrastructure, including any technology that can deliver broadband to residential and institutional customers. The bill requires that retail broadband services must be provided by a private entity, which has entered into a use agreement with a governmental unit that owns the infrastructure. The bill also establishes terms and conditions for the administration of the fund. The bill, in its current form, does not contain an appropriation or other source of money for the broadband revolving loan fund.

MSG:cs

Senate Counsel, Research, and Fiscal Analysis

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate
State of Minnesota

S.F. No. 1370 - Standardized Telecommunications Provider Contracts in Lieu of Tariffs

Author: Senator Steve Kelley

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890)MG

Date: March 11, 2005

The bill directs the Public Utilities Commission to develop standardized contracts for the provision of residential and business telephone service in Minnesota by July 1, 2006. Providers of such service may choose to provide service under the terms of the contract in lieu of a tariff filed at the commission if a tariff would otherwise be required under Minnesota Statutes, Chapter 237. Such contracts must comply with all Minnesota laws governing contracts and provide for specified consumer protections including, but not limited to, clear and detailed disclosure of rates and terms of service, provision of a service trial period, confirmation by consumer of changes in the terms and conditions, complaint resolution guidelines and mandatory arbitration, and compliance with the federal Communications Assistance for Law Enforcement Act.

The contracts must also provide for reasonable and appropriate contributions to the 911 emergency response system, the telephone assistance plan and telecommunications access Minnesota programs, telecommunications regulatory fees, as well as reasonable intercarrier compensation, and financial support for the public switched telephone network.

Specific contracts developed under this bill must be filed with the Commissioner of Commerce ten days prior to being used by a service provider to offer services under the contract. The Commissioner of Commerce is directed to rescind the ability of a service provider to offer services under a contract upon finding of violation(s) of the contract, if doing so is in the public interest.

MSG:cs

Senators Kelley, Anderson, Stumpf and Kubly introduced--

S.F. No. 1225: Referred to the Committee on Jobs, Energy and Community Development.

A bill for an act

relating to communications; creating a broadband revolving loan fund; proposing coding for new law in Minnesota Statutes, chapter 446A.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [446A.086] [BROADBAND REVOLVING LOAN FUND.]

Subdivision 1. [DEFINITIONS.] (a) The definitions in this subdivision apply to this section.

(b) "Authority" means the Minnesota Public Facilities Authority.

(c) "Broadband" means data telecommunication that is delivered at a minimum speed of 100 megabits per second for residential users and one gigabit per second for business and institutional users.

(d) "Commissioner" means the commissioner of employment and economic development.

(e) "Governmental unit" means a state agency, home rule charter or statutory city, county, municipal utility, or other governmental subdivision.

(f) "Loan" means financial assistance provided for all or part of the cost of a project, including money disbursed in anticipation of reimbursement or repayment, loan guarantees, lines of credit, credit enhancements, equipment financing leases, bond insurance, or other forms of financial assistance.

Subd. 2. [PURPOSE.] The purpose of the broadband revolving

loan fund is to provide loans for local communications infrastructure, including any technology that can deliver broadband to residential and institutional customers. The technology that delivers broadband includes, but is not limited to, fiber-optic cable, coaxial cable, copper wire, wireless systems, satellite systems, and electrical lines.

Subd. 3. [ESTABLISHMENT OF FUND.] A broadband revolving loan fund is established to make loans to government units for the purposes described in subdivision 2.

Subd. 4. [ELIGIBLE PROJECTS.] Loans may be made only for broadband infrastructure projects owned by a governmental unit and approved by the commissioner. The provision of retail broadband service to residential and institutional customers must be provided by a private entity capable of providing retail broadband services, including voice, video, and data services. The retail broadband service provider must enter into a use agreement with the governmental unit that owns the infrastructure.

Subd. 5. [APPLICATIONS.] Applicants for loans must submit an application to the authority on forms provided by the authority. The applicant must provide the following information:

(1) the estimated cost of the project and the amount of the loan sought;

(2) other possible sources of funding in addition to loans sought from the broadband revolving loan fund;

(3) the proposed methods and sources of funds to be used for repayment of loans received;

(4) information showing the financial status and ability of the borrower to repay loans;

(5) information showing that the demand exists for broadband services; and

(6) information showing the experience of the retail broadband service provider.

Subd. 6. [CERTIFICATION OF PROJECTS.] The commissioner shall consider the following information when evaluating projects for funding by the authority:

(1) a description of the nature and purpose of the proposed broadband project, including an explanation of the need for the project and the reasons why it is in the public interest;

(2) the estimated cost of the project and the amount of loans sought;

(3) proposed sources of funding in addition to loans sought from the broadband revolving loan fund;

(4) the viability of the technology that will deliver the broadband service; and

(5) the viability of the retail broadband service provider that will provide retail broadband services using the infrastructure.

Subd. 7. [LOAN CONDITIONS.] When making loans from the broadband revolving loan fund, the authority shall engage in prior consultation with the Department of Commerce. Loans must:

(1) bear interest at or below market rates;

(2) have a repayment term not longer than 15 years;

(3) be fully amortized no later than 15 years after project completion; and

(4) be subject to repayment of principal and interest beginning not later than three years after the infrastructure financed with a loan has been completed.

Subd. 8. [OPEN ACCESS.] Access to the infrastructure financed in whole or in part by a loan under this section must be nonexclusive to a provider and open to all qualified providers.

Senators Kelley, Ourada, Gaither, Kubly and Metzen introduced--

S.F. No. 1370: Referred to the Committee on Jobs, Energy and Community Development.

A bill for an act

relating to telecommunications; providing for standardized provider contracts; proposing coding for new law in Minnesota Statutes, chapter 237.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [237.82] [CONTRACT FOR THE PROVISION OF SERVICE.]

Subdivision 1. [COMMISSION TO DEVELOP STANDARDS.] (a) By July 1, 2006, the commission shall, by rule or order, develop standards for contracts under which a service provider may choose to offer service to Minnesota residential and business customers. A contract under this section may be offered in lieu of a tariff filed at the commission if a tariff would otherwise be required under this chapter.

(b) For the purposes of this section, "service provider" means a provider of real time, two-way voice service using numbers allocated for Minnesota assigned by the North American Numbering Plan Administration to interconnect with the public switched telephone network.

Subd. 2. [CONSUMER PROTECTION REQUIREMENTS.] A contract offered under this section must comply with all Minnesota laws governing contracts and provide at least the following consumer protections:

(1) detailed disclosure of the rates and terms of service, including activation or initiation fees; monthly access fees or

base charges; any required contract term; early termination fees; whether prices or benefits apply only for a limited time, and if so, the fees or charges to be paid for the remainder of the contract term; and whether any additional taxes, fees, or surcharges apply;

(2) a trial period for new service and clear disclosure of the terms and conditions of the trial period;

(3) confirmation by the customer of changes in material terms and conditions of service and the customer's right to terminate for those changes;

(4) a clear and separate identification of telephone company charges from government-imposed taxes and fees on billing statements;

(5) easy access to customer service;

(6) specific complaint resolution guidelines and a prohibition of mandatory arbitration requirements;

(7) protection of the customer's personal information and privacy; and

(8) compliance with the federal Communications Assistance for Law Enforcement Act.

Subd. 3. [OTHER REQUIREMENTS.] In addition to the requirements for the protection of consumers under subdivision 2, the contract must provide for reasonable and appropriate contributions for the 911 emergency response system; the telephone assistance plan and telecommunications access Minnesota programs; and telecommunications regulatory fees, as well as for reasonable intercarrier compensation and financial support for the public switched telephone network.

Subd. 4. [ELECTION REQUIREMENTS AND REGULATORY FORBEARANCE.] For each type of service provider that is subject to this chapter, the commission's rule or order under this section must specify the requirements under which that type of provider may elect to offer service under a contract under this section and the regulatory requirements under this chapter, such as tariff filing and approval, for which the commission would forbear from applying to service offered under the contract.

Subd. 5. [CONTRACT USE; VIOLATION.] (a) A specific contract developed under subdivision 1 must be filed with the commissioner of commerce ten days prior to being used by a service provider to offer service under the contract. The commissioner is initially responsible for resolving disputes arising under contracts developed under this section, subject to appeal to the commission.

(b) The commission shall rescind the ability of a service provider to offer service under a contract pursuant to this section upon a finding of a violation or violations of this section or the contract, if the commission determines that doing so is in the public interest.

Senators Sparks, Senjem and Foley introduced--

S.F. No. 927: Referred to the Committee on Commerce.

A bill for an act

relating to commerce; regulating false and deceptive commercial electronic mail messages; prescribing criminal penalties; providing remedies; proposing coding for new law in Minnesota Statutes, chapter 325F.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [325F.696] [DEFINITIONS.]

Subdivision 1. [SCOPE.] For the purposes of sections 325F.696 to 325F.6991, the terms in this section have the meanings given them.

Subd. 2. [COMMERCIAL ELECTRONIC MAIL MESSAGE.] "Commercial electronic mail message" means any electronic mail message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service, including content on an Internet Web site operated for a commercial purpose, but does not include a transactional or relationship message. The inclusion of a reference to a commercial entity or a link to the Web site of a commercial entity does not, by itself, cause that message to be treated as a commercial electronic mail message for the purpose of this section if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service.

Subd. 3. [COMPUTER.] "Computer" means an electronic device that performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses. "Computer"

includes, but is not limited to, all input, output, processing, storage, computer program, or communication facilities that are connected or related in a computer system or network to an electronic device of that nature.

Subd. 4. [COMPUTER NETWORK.] "Computer network" means a set of related and remotely connected computers and communication facilities that includes more than one computer system that has the capability to transmit among the connected computers and communication facilities through the use of computer facilities.

Subd. 5. [COMPUTER SYSTEM.] "Computer system" means a computer and related devices, whether connected or unconnected, including, but not limited to, data input, output, and storage devices, data communication links, and computer programs and data that make the system capable of performing specified special purpose data processing tasks.

Subd. 6. [DOMAIN NAME.] "Domain name" means any alphanumeric designation that is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.

Subd. 7. [ELECTRONIC MAIL.] "Electronic mail" means an electronic message that is transmitted between two or more telecommunications devices or electronic devices capable of receiving electronic messages, whether or not the message is converted to hard copy format after receipt, and whether or not the message is viewed upon the transmission or stored for later retrieval. "Electronic mail" includes electronic messages that are transmitted through a local, regional, or global computer network.

Subd. 8. [ORIGINATING ADDRESS.] "Originating address" means the string of characters used to specify the source of any electronic mail message.

Subd. 9. [RECEIVING ADDRESS.] "Receiving address" means the string of characters used to specify a recipient with each receiving address creating a unique and separate recipient.

Subd. 10. [ELECTRONIC MAIL MESSAGE.] "Electronic mail message" means each electronic mail addressed to a discrete addressee.

Subd. 11. [ELECTRONIC MAIL SERVICE PROVIDER.] "Electronic mail service provider" means any person, including an Internet service provider, that is an intermediary in sending and receiving electronic mail and that provides to the public electronic mail accounts or online user accounts from which electronic mail may be sent.

Subd. 12. [HEADER INFORMATION.] "Header information" means the source, destination, and routing information attached to an electronic mail message, including the originating domain name, originating address, and technical information that authenticates the sender of an electronic mail message for computer network security or computer network management purposes.

Subd. 13. [INITIATE THE TRANSMISSION; INITIATED.] "Initiate the transmission" or "initiated" means to originate or transmit a commercial electronic mail message or to procure the origination or transmission of that message, regardless of whether the message reaches its intended recipients, but does not include actions that constitute routine conveyance of the message.

Subd. 14. [INTERNET.] "Internet" means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to this protocol, to communication information of all kinds by wire or radio.

Subd. 15. [INTERNET PROTOCOL ADDRESS.] "Internet protocol address" means the string of numbers by which locations on the Internet are identified by routers or other computers connected to the Internet.

Subd. 16. [MATERIALLY FALSIFY.] "Materially falsify" means to alter or conceal in a manner that would impair the ability of

a recipient of an electronic mail message, an electronic mail service provider processing an electronic mail message on behalf of a recipient, a person alleging a violation of section 325F.697, or a law enforcement agency to identify, locate, or respond to the person that initiated the electronic mail message or to investigate an alleged violation of this section.

Subd. 17. [MULTIPLE.] "Multiple" means more than ten commercial electronic mail messages during a 24-hour period, more than 100 commercial electronic mail messages during a 30-day period, or more than 1,000 commercial electronic mail messages during a one-year period.

Subd. 18. [RECIPIENT.] "Recipient" means a person who receives a commercial electronic mail message at any one of the following receiving addresses:

(1) a receiving address furnished by an electronic mail service provider that bills for furnishing and maintaining that receiving address to a mailing address within this state;

(2) a receiving address ordinarily accessed from a computer located within this state or by a person domiciled within this state; or

(3) any other receiving address with respect to which this section can be imposed consistent with the United States Constitution.

Subd. 19. [ROUTINE CONVEYANCE.] "Routine conveyance" means the transmission, routing, relaying, handling, or storing, through an automated technical process, of an electronic mail message for which another person has identified the recipients or provided the recipient addresses.

Subd. 20. [TRANSACTIONAL OR RELATIONSHIP MESSAGE.] "Transactional or relationship message" means an electronic mail message the primary purpose of which is to do any of the following:

(1) facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(2) provide warranty information, product recall

information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(3) provide notification concerning a change in the terms or features of; a change in the recipient's standing or status with respect to; or, at regular periodic intervals, account balance information or other type of account statement with respect to a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

(4) provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(5) deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

Sec. 2. [325F.697] [FALSE, MISLEADING, OR DECEPTIVE COMMERCIAL ELECTRONIC MAIL MESSAGES PROHIBITED.]

No person, with regard to commercial electronic mail messages sent from or to a computer in this state, shall do any of the following:

(1) knowingly use a computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients or any electronic mail service provider, as to the origin of those messages;

(2) knowingly and materially falsify header information in multiple commercial electronic mail messages and purposely initiate the transmission of those messages;

(3) knowingly register, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names and purposely initiate the transmission of multiple commercial electronic mail messages from one, or any combination, of those accounts or domain names;

(4) knowingly falsely represent the right to use five or more Internet protocol addresses and purposely initiate the transmission of multiple commercial electronic mail messages from those addresses.

Sec. 3. [325F.698] [ILLEGAL TRANSMISSION OF MULTIPLE MESSAGES; CRIMINAL PENALTIES.]

(a) Whoever violates section 325F.697 is guilty of illegally transmitting multiple commercial electronic mail messages. Except as otherwise provided in paragraph (b) or section 325F.699, subdivision 3, illegally transmitting multiple commercial electronic mail messages is a misdemeanor.

(b) Illegally transmitting multiple commercial electronic mail messages is a gross misdemeanor if any of the following apply:

(1) regarding a violation of section 325F.697, clause (3), the offender, using information that materially falsifies the identity of the actual registrant, knowingly registers for 20 or more electronic mail accounts or online user accounts or ten or more domain names, and purposely initiates, or conspires to initiate, the transmission of multiple commercial electronic mail messages from the accounts or domain names;

(2) regarding any violation of section 325F.697, the volume of commercial electronic mail messages the offender transmitted in committing the violation exceeds 250 during any 24-hour period, 2,500 during any 30-day period, or 25,000 during any one-year period;

(3) regarding any violation of section 325F.697, during any one-year period the aggregate loss to the victim or victims of the violation is $500 or more, or during any one-year period the aggregate value of the property or services obtained by any offender as a result of the violation is $500 or more;

(4) regarding any violation of section 325F.697, the offender committed the violation with three or more other persons with respect to whom the offender was the organizer or leader of the activity that resulted in the violation;

(5) regarding any violation of section 325F.697, the

offender knowingly assisted in the violation through the provision or selection of electronic mail addresses to which the commercial electronic mail message was transmitted, if that offender knew that the electronic mail addresses of the recipients were obtained using an automated means from an Internet Web site or proprietary online service operated by another person, and that Web site or online service included, at the time the electronic mail addresses were obtained, a notice stating that the operator of that Web site or online service will not transfer addresses maintained by that Web site or online service to any other party for the purposes of initiating the transmission of, or enabling others to initiate the transmission of, electronic mail messages; or

(6) regarding any violation of section 325F.697, the offender knowingly assisted in the violation through the provision or selection of electronic mail addresses of the recipients obtained using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations.

Sec. 4. [325F.699] [UNAUTHORIZED ACCESS TO A COMPUTER; CRIMINAL PENALTIES.]

Subdivision 1. [PROHIBITION.] No person, with regard to commercial electronic mail messages sent from or to a computer in this state, shall knowingly access a computer without authorization and purposely initiate the transmission of multiple commercial electronic mail messages from or through the computer.

Subd. 2. [GROSS MISDEMEANOR.] Except as otherwise provided in subdivision 3, whoever violates subdivision 1 is guilty of unauthorized access of a computer, a gross misdemeanor.

Subd. 3. [FELONY.] Illegally transmitting multiple commercial electronic mail messages and unauthorized access of a computer in violation of this section are felonies if the offender previously has been convicted of a violation of this section, or a violation of a law of another state or the United States regarding the transmission of electronic mail messages or

unauthorized access to a computer, or if the offender committed the violation of this section in the furtherance of a felony.

Sec. 5. [325F.6991] [CIVIL ACTIONS.]

(a) The attorney general or an electronic mail service provider that is injured by a violation of this section may bring a civil action in district court seeking relief from any person whose conduct violated section 325F.697. The civil action may be commenced at any time within one year of the date after the act that is the basis of the civil action.

(b) In a civil action brought by the attorney general for a violation of section 325F.697, the court may award temporary, preliminary, or permanent injunctive relief. The court also may impose a civil penalty against the offender, as the court considers just, in an amount that is the lesser of: (1) $25,000 for each day a violation occurs; or (2) not less than $2 but not more than $8 for each commercial electronic mail message initiated in violation of this section.

(c) In a civil action brought by an electronic mail service provider for a violation of section 325F.697, the court may award temporary, preliminary, or permanent injunctive relief, and also may award damages in an amount equal to the greater of the following:

(1) the sum of the actual damages incurred by the electronic mail service provider as a result of a violation of this section, plus any receipts of the offender that are attributable to a violation of this section and that were not taken into account in computing actual damages;

(2) statutory damages, as the court considers just, in an amount that is the lesser of: (i) $25,000 for each day a violation occurs; or (ii) not less than $2 but not more than $8 for each commercial electronic mail message initiated in violation of this section.

(d) In assessing damages, the court may consider whether the offender has established and implemented, with due care, commercially reasonable practices and procedures designed to effectively prevent the violation, or the violation occurred

despite commercially reasonable efforts to maintain the practices and procedures established.

(e) Equipment, software, or other technology of a person who violates this section that is used or intended to be used in the commission of a violation of this section, and any real or personal property that constitutes or is traceable to the gross proceeds obtained from the commission of a violation of this section, is contraband and is subject to seizure and forfeiture pursuant to section 609.531.

(f) The attorney general may bring a civil action, pursuant to the "CAN-SPAM Act of 2003," Public Law 108-187, 117 Stat. 2699, United States Code, title 15, section 7701 et seq., on behalf of the residents of the state in a district court of the United States that has jurisdiction for a violation of the CAN-SPAM Act of 2003, but the attorney general shall not bring a civil action under both this paragraph and paragraph (a). If a federal court dismisses a civil action brought under this section for reasons other than upon the merits, a civil action may be brought under this section in the appropriate district court of this state.

(g) Nothing in sections 325F.696 to 325F.6991:

(1) requires an electronic mail service provider to block, transmit, route, relay, handle, or store certain types of electronic mail messages;

(2) prevents or limits, in any way, an electronic mail service provider from adopting a policy regarding electronic mail, including a policy of declining to transmit certain types of electronic mail messages or from enforcing such policy through technical means, through contract, or pursuant to any remedy available under any other federal, state, or local criminal or civil law; and

(3) renders lawful any policy adopted under clause (2) that is unlawful under any other law.

Sec. 6. [EFFECTIVE DATE; APPLICATION.]

This act is effective August 1, 2005. Sections 3 and 4 apply to crimes committed on or after that date.

Senator ..... moves to amend S.F. No. 1225 as follows:

Page 3, after line 26, insert:

"Sec. 2. [APPROPRIATION; BROADBAND REVOLVING LOAN FUND.]

$..... is appropriated from the bond proceeds fund to the public facilities authority for deposit in the broadband revolving loan fund created by Minnesota Statutes, section 446A.086, for the purposes of the fund.

Sec. 3. [BOND AUTHORIZATION.]

To provide the money appropriated in this act from the bond proceeds fund, the commissioner of finance shall sell and issue bonds of the state in an amount up to $..... in the manner, upon the terms, and with the effect prescribed by Minnesota Statutes, sections 16A.631 to 16A.675, and by the Minnesota Constitution, article XI, sections 4 to 7."

Amend the title as follows:

Page 1, line 3, after the semicolon, insert "authorizing bonds; appropriating money;"