4000

DEPARTMENT OF EDUCATION

Third-Party Access to the Department's Information Technology Systems and Notice of Criminal Penalties for Misuse of Access Devices

AGENCY: Federal Student Aid, Department of Education.

ACTION: Notice.

SUMMARY: The U.S. Department of Education (Department) outlines the requirements for third-party access to the Department's Information Technology (IT) systems and establishes criminal penalties for misuse of access devices. Specifically, this notice sets forth the definition of an access device, the terms of service, the Code of Conduct, and information security standards, and provides notice of related criminal penalties.

DATES: This notice is applicable [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Michael Ruggless, Federal Student Aid, 830 First Street, NE, Union Center Plaza, room 114B4, Washington, DC 20202-5345. Telephone: (202) 377-4098. Email: Michael.Ruggless@ed.gov.

Tamy Abernathy, Office of Postsecondary Education, 400 Maryland Avenue, SW, 2C-129, Washington, DC 20202. Telephone: (202) 453-5970. Email: Tamy.Abernathy@ed.gov.

If you use a telecommunications device for the deaf (TDD) or a text telephone (TTY), call the Federal Relay

Service, toll free, at 1-800-877-8339.

SUPPLEMENTARY INFORMATION:

The Stop Student Debt Relief Scams Act of 2019 (STOP Act) amended sections 141, 485B, and 490 of the Higher Education Act of 1965, as amended (HEA), on December 22, 2020, to prevent and address the improper use of access devices issued by the Department and establish criminal penalties for improper use. (Pub. L. 116-251; 134 Stat. 1129-1132). Section 485B(e) of these HEA amendments includes provisions for the prevention of improper access to the Department's systems. Section 490(e) of these HEA amendments explicitly makes unauthorized access to the Department's IT systems and the misuse of identification devices issued by the Department a criminal act. Criminal penalties associated with the STOP Act are applicable one day after the date of publication of this notice. All other actions and information pursuant to these HEA amendments contained in this notice are applicable upon publication.

The Department establishes, pursuant to section 2(b) of the STOP Act, the following definition of an access device, terms of service, information security standards, and Code of Conduct.

Definition of Access Device

An access device, as defined in 18 U.S.C. 1029(e)(1), means any--

(a) Card;

(b) Plate;

(c) Code;

(d) Account number;

(e) Electronic serial number;

(f) Mobile identification number;

(g) Personal identification number;

(h) Other telecommunications service, equipment, or instrument identifier; or

(i) Other means of account access that can be used alone or in conjunction with another access device—

(1) To obtain money, goods, services, or any other thing of value; or

(2) To initiate a transfer of funds (other than a transfer originated solely by paper instrument).

Terms of Service

An authorized user must abide by the Code of Conduct and Information Security Standards for Department systems.

Acceptable Use of Systems

(a) A person or entity may be granted access to, and use and share, the Department's assets, data, information resources, and information systems (collectively, the Department's information systems) only if the person or entity is an "authorized user" under paragraph (b) and only to the extent otherwise authorized pursuant to this section.

(b) A person or entity may be granted access to the Department's information systems as an authorized user if the person or entity has a bona fide "need to know" the information or data contained in the Department's information systems and they are--

(1) A student, borrower, or parent;

(2) A guaranty agency, eligible lender, eligible institution, or a third-party organization acting on behalf of a guaranty agency, eligible lender, or eligible institution that complies with Federal law and requirements applicable to the Department's information systems; or

(3) A licensed attorney representing a student, borrower, or parent, or another individual who works for a Federal, State, local, or Tribal government or agency, or for a nonprofit organization, providing financial or student loan repayment counseling to a student, borrower, or parent, if—

(i) The attorney or other individual has never engaged in unfair, deceptive, or abusive practices, as determined by the Department;

(ii) The attorney or other individual does not work for an entity that has engaged in unfair, deceptive, or abusive practices (including an entity that is owned or operated by a person or entity that engaged in such practices), as determined by the Department;

(iii) System access is provided only through a

separate point of entry issued to the attorney or other individual; and

(iv) The attorney or other individual has written consent from the relevant student, borrower, or parent to access the system.

(c) To access the Department's information systems, an authorized user must—

(1) Read, understand, and sign the information system-specific Rules of Behavior;

(2) Have valid and current access authorization issued by the Department;

(3) Access the Department's information systems using an access device issued by the Department to the authorized user, and may not use an access device issued by the Department to a student, borrower, or parent. A student, borrower, or parent, including through a power of attorney, may not authorize a third party to use their access device; and

(4) Comply with the terms of service, information security standards, and Code of Conduct.

(d) No person or entity may access the Department's information systems for the purpose of assisting a student in managing loan repayment or applying for any repayment plan, consolidation loan, or other benefit authorized under title IV of the HEA, except as permitted under this "Acceptable Use of Systems."

Criminal Penalties

Section 2 of the STOP Act, Pub. L. 116-251, amended section 490 of the HEA (20 U.S.C 1097), by adding paragraph (e), which makes it a crime to knowingly use an access device that was issued to another person or obtained by fraud or false statement to access Department information technology systems for commercial advantage, private financial gain, criminal activity, or wrongful act violating United States or State law. A violator is subject to criminal penalties that include a fine of not more than $20,000, imprisonment for not more than five years, or both, beginning one day after the date of publication of this notice.

Code of Conduct

This Code of Conduct identifies the acceptable rules of behavior for accessing the Department's information systems. Upon accessing the Department's information systems, all users will receive a notification warning banner similar to the following that requires them to acknowledge and agree to the Code of Conduct prior to being allowed further access:

"You are accessing a U.S. Federal Government computer system intended to be solely accessed by individual users expressly authorized to access the system by the U.S. Department of Education. Usage may be monitored, recorded, and/or subject to audit. For security purposes, and in

order to ensure that the system remains available to all expressly authorized users, the U.S. Department of Education monitors the system to identify unauthorized users. Anyone using this system expressly consents to such monitoring and recording. Unauthorized use of this information system is prohibited and subject to criminal and civil penalties. Except as expressly authorized by the U.S. Department of Education, unauthorized attempts to access, obtain, upload, modify, change, and/or delete information on this system are strictly prohibited and are subject to criminal prosecution under 18 U.S.C. 1030, and other applicable statutes, which may result in fines and imprisonment. This system may contain Personally Identifiable Information (PII), as defined by the Privacy Act of 1974, or other Controlled Unclassified Information as defined by 32 CFR 2002.

For purposes of this system, unauthorized access includes, but is not limited to—

(a) Any access by an employee or agent of a commercial entity, or other third party, who is not the individual user, for purposes of commercial advantage or private financial gain (regardless of whether the commercial entity or third party is providing a service to an authorized user of the system); and

(b) Any access in furtherance of any criminal or tortious act in violation of the Constitution or laws of

the United States or any State.

If system monitoring reveals information indicating possible criminal activity, such evidence may be provided to law enforcement personnel. These Rules of Behavior identify responsibilities and expectations for all individuals accessing Federal Student Aid (FSA) systems. By accepting, you confirm that you have reviewed, acknowledge, and agree to the following Rules of Behavior:

(a) You must protect all of the Department's information systems, including the Department's data and information in your possession, from access by, or disclosure to, unauthorized individuals or entities.

(b) Your User ID, password, and other credentials are unique and only assigned to the specified authorized user.

(1) Your User ID, password, and other credentials serve as an electronic signature for signing fiduciary documents committing you to financial obligations.

(2) Your User ID, password, and other credentials are for official Department business only.

(c) You must never give your User ID, password, or other credentials to another person, including your supervisor(s). Any information retrieved from the Department's information systems may be shared only with individuals expressly authorized to receive this information.

(d) You must access only systems, networks, data,

control information, and software for which you have been authorized by the U.S. Department of Education.

(e) If you are a third party representing an authorized user under paragraph (b) of the "Acceptable Use of Systems," you must be issued your own unique User ID, password, or credentials; at no time is a third party authorized to use another individual's unique User ID, password, or credentials. A user may not authorize a third party to use their User ID, password, or credentials, including through a power of attorney.

(f) You are individually responsible for ensuring that data/information obtained from the Department's information systems is not used improperly. A legitimate reason must be present to view data/information contained within the Department's information systems.

(g) You must change your password immediately and notify the appropriate security personnel if your password is compromised, or someone else knows your password.

(h) You must properly encrypt (or password protect) all electronic files when transmitting data via email. Passwords must be sent separately (not in the same transmission or transmission channel).

(i) All paper documents containing PII or Controlled Unclassified Information must be labeled and stored in a secure environment, to which only authorized personnel have access.

(j) You must inform or contact the organization that granted initial access when access to an FSA system is no longer required or access changes because of changes in job responsibilities or termination of employment.

(k) You must remain current on all required training, including security training (at least annually).

(l) You must not download or store the Department's information systems information or data on unsecure/public computers or portable devices.

(m) If you have Title IV loans, they must be in good standing. If you have a loan that goes into default, your access to the Department's information systems will be revoked."

Information Security Standards

In addition to requirements identified in the Terms of Service and Code of Conduct, individuals accessing Department of Education information systems must comply with the following requirements:

(a) A third party accessing the Department's information systems, on behalf of an authorized user, must ensure proper control and handling of Controlled Unclassified Information (CUI), which includes data commonly known as PII, Sensitive Personally Identifiable Information (SPII) and CUI, residing on their computer, on removable media, and on paper documents.

(b) A third party that handles CUI must do so in

accordance with Executive Order 13556, 32 CFR 2002 – Controlled Unclassified Information, and the CUI Registry.

(c) The third party must ensure data at rest that contains CUI is encrypted using validated FIPS 140-2 encryption in any and all third-party computing environments where data is housed and/or stored.

(d) The third party must consider data at rest to include data that reside in databases, file systems, information technology systems, applications, personal computers (desktops and laptops and portable electronic devices [PEDs] and mobile electronic devices and personal data assistants [PDAs]) and other structured storage devices (USB flash drives, memory cards, external hard drives, writeable CDs, and DVDs) that are not in transit.

(e) The third party must ensure the integrity and confidentiality of the information and protect against any reasonably anticipated security threats or unauthorized uses or disclosures of the information.

If, at any time, CUI is provided to or viewed by unauthorized individual(s), a breach report is required by the third party. A breach report must be submitted to the Department of Education Security Operations Center (EDSOC), email to EDSOC@ed.gov. EDSOC may also be contacted by phone at (202) 245-6550.

A Breach or Data Breach is an incident that includes the loss of control, compromise, unauthorized disclosure,

unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose OMB M-17-12, p. 9. An occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves PII. Breaches include cyber incidents, as well as the loss or theft of physical documents or portable electronic storage media, inadvertent disclosure of PII on a public website, an oral disclosure to a person not authorized to receive that information, or an authorized user accessing PII for an unauthorized purpose, etc.

Accessible Format: On request to one of the program contact persons listed under FOR FURTHER INFORMATION CONTACT, individuals with disabilities can obtain this document in an accessible format. The Department will provide the requestor with an accessible format that may include Rich Text Format (RTF) or text format (txt), a thumb drive, an MP3 file, braille, large print, audiotape, or compact disc, or other accessible format.

Electronic Access to This Document: The official version of this document is the document published in the *Federal Register*. You may access to the official edition of the *Federal Register* and the Code of Federal Regulations at www.govinfo.gov. At this site you can view this document,

as well as all other documents of this Department published in the *Federal Register*, in text or Portable Document Format (PDF). To use PDF you must have Adobe Acrobat Reader, which is available free at the site.

You may also access documents of the Department published in the *Federal Register* by using the article search feature at www.federalregister.gov. Specifically, through the advanced search feature at this site, you can limit your search to documents published by the Department.

Program Authority: 20 U.S.C 1001; 20 U.S.C. 1018; 20 U.S.C. 1092b; and 20 U.S.C. 1097.

Richard Cordray,
Chief Operating Officer,
Federal Student Aid.

[FR Doc. 2021-19536 Filed: 9/9/2021 8:45 am; Publication Date: 9/10/2021]