

FTC SAFEGUARDS RULE

Gramm-Leach-Bliley

Act Effective 5/23/2003

Introduction

The purpose of the FTC Safeguards Rule is to:

- Ensure the security and confidentiality of customer information.
 - Customer information is defined as any record containing nonpublic personal information such as a social security number, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of UOTP or its affiliates.
- Protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.
- This rule is governed by the Federal Trade Commission and is required by the Gramm-Leach-Bliley Act that was signed into law on November 12, 1999.

For more information, go to: <https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act>

Protected Customer Information

The privacy rule limits the use and disclosure of customer information. View the Family Educational Rights and Privacy Act (FERPA) at this website: <https://potomac.edu/students/office-of-the-registrar/>

Covered Entities: Non-directory information such as social security numbers, grades, schedules, GPAs, bank account numbers, and academic standing.

Practical Tips for Safeguarding Customer Information

- Do not leave confidential data unattended or visible to others.
- Shred and never recycle documents containing confidential customer information such as a social security number.
- Secure all daily work in locked file cabinets or drawers.
- Protect secured areas – lock all doors, and never loan your key.
- Talk quietly when discussing confidential or private information with a customer.
 - Avoid the use of names or other identifying information whenever possible.

Practical Tips for Safeguarding Customer Information

- Sensitive information should not be sent to remote printers or photocopiers where access is uncontrolled. Nor should it be faxed where the physical security of the receiver is unknown.
 - Include a confidential statement on your fax transmittal sheet that information sent to the incorrect destination be destroyed and requesting notification to the sender of such errors.
 - Do not dispose of documents containing nonpublic information in wastebaskets, or recycling bins; instead, shred or otherwise destroy them before discarding.
- Sensitive information should never be left on voicemail or answering machines.
- Avoid using nonpublic information via e-mail.
- Use password-activated screensavers.

Policies and Guidelines

UOTP safeguards customers' information by adhering to the following policies and guidelines:

- Federal Educational Rights and Privacy Act (FERPA) - <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- State and University policies on Records Retention and Disposition - <https://potomac.edu/students/office-of-the-registrar/>
- University Financial Policies - <https://potomac.edu/students/course-catalog/>
- State of Virginia Information Technology Policies and Guidelines - <https://www.vita.virginia.gov/policy--governance/policies-standards--guidelines/>
- State and University Human Resources Policies and Guidelines –refer to the Employee and Faculty Handbooks.

Comments/Questions

Please forward any comments or questions to the Qualified Individual:

Mr. Mark Jiidee

Executive Director of IT Systems and Facilities

1401 H Street, N.W., Suite 100, Washington, D.C. 20005

P: 202-274-1789

mark.jiidee@potomac.edu



Potomac.edu