

Viterbo University

Identity Theft Prevention Program

Viterbo University is dedicated to protecting all data that it receives and maintains in its files and databases. The University is also committed to providing resources to members of the University community to help them protect themselves from being victims of identity theft.

Prevention and Mitigation

Viterbo is dedicated to the prevention of identity theft through the official adoption and implementation of the Family Education Rights and Privacy Act (FERPA). Viterbo's FERPA policy is available at <https://www4.viterbo.edu/registrar/ferpa> and applied to the information obtained, stored and used within the University's database.

In addition to the adoption and implementation of the FERPA policy, Viterbo's Instructional and Information Technology department has implemented security profiles for each office on campus and has initiated secure access to the University's database by students or employees through the internet or intranet. Students and employees are encouraged to change their electronic access passwords regularly, and to not leave their computers unattended without securing them.

Viterbo is dedicated to mitigating identity theft by regularly informing students and employees of the potential problems associate with identity theft. In addition, seminars are held for students and employees, to discuss issues surrounding identify theft and how to prevent and deal with any occurrences.

There are many identity theft resources available to students and employees:

The Federal Trade Commission has an excellent web site dedicated to "Deterring, Detecting and Defending" against identity theft.

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

This is the Federal Trade Commission's identity theft webpage.

Additional web sites include:

<http://www.onguardonline.gov/>

This website provides information to help individuals guard against internet fraud, secure computers, and protect personal information.

<https://www.annualcreditreport.com/cra/index.jsp>

This website can be used to obtain credit reports.

<http://www.privacyrights.org/>

This website contains data loss statistical information.

<https://www.microsoft.com/en-us/security>

This is Microsoft's security homepage.

Detection

Viterbo University is dedicated to the identification and prosecution of potential identity theft attempts with the incorporation of the following “Red Flag” actions. “Red Flags” are patterns, practices or specific activities that indicate the possible existence of identity theft in connection with Viterbo students, employees and vendors. Below are examples of “red flags”

- A student application appears to have been forged, altered, or destroyed and reassembled
- Documents provided for identification of students or employees appearing altered or forged
- A photograph or information on an ID is inconsistent with appearance or information provided by a student or employee
- The Social Security number supplied by a student or employee is the same as that submitted by another person, or does not agree with the Social Security Administration Verification Webpage
- The address or telephone number supplied by a student applicant is the same or similar to the account number or telephone number submitted by an unusually large number of other persons
- Viterbo is notified that the student is not receiving account statements

If Viterbo should identify a “Red Flag” issue when a student account or employee personnel record is established in its database, an investigation should immediately occur by the office obtaining the information. If the information appears to be fraudulent, the office should notify the Vice President of Finance and Administration. The Vice President of Finance and Administration will investigate the matter and then determine one of the following actions to be considered:

1. Closing the investigation if there is no conclusion of fraud
2. If fraud is suspected:
 - a. Monitoring of the student or employee account is fraud if suspected
 - b. Notifying the affected student or employee
 - c. Encouraging the student or employee to change electronic access passwords
 - d. Notifying law enforcement