Walla Walla University
SEVENTH-DAY ADVENTIST HIGHER EDUCATION

Identity Theft Rules &
Identity Theft Prevention Program

I. IDENTITY THEFT RULES:

The Identity Theft[1] Rules, adopted as 16 CFR 681, require any entity where there is a risk of identity theft, to develop and implement an Identity Theft Prevention Program. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission (FTC), the Office of the Comptroller of the Currency, and the Office of Thrift Supervision issued the rules which became effective on November 1, 2008.

The Identity Theft Rules are divided into the following three areas:

(1) § 681.1 Duties of users of consumer reports regarding address discrepancies.

(2) § 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

(3) § 681.3 Duties of card issuers regarding changes of address.

All of the duties contained in these regulations § 681.1, § 681.2 and § 681.3 which are applicable to Walla Walla University are incorporated into the "Identity Theft Prevention Program" which is outlined in Section II. The detailed regulations for § 681.1, § 681.2 and § 681.3 are summarized as follows:

§ 681.1 Duties of users of consumer reports regarding address discrepancies.

Requires the development and implementation of reasonable policies and procedures to handle notices of address discrepancies received from consumer credit companies and companies that perform background checks.

§ 681.1 applies to Walla Walla University in the following areas:

(1) Student Financial Services runs credit reports on students, particularly with respect to institutional loans that are past-due.

(2) Human Resources performs background checks for potential employment.

---

[1] "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority. See 16 C.F.R. § 603.2(a). "Identifying information" means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any –
(1) Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
(3) Unique electronic identification number, address, or routing code; or
(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e))."
See 16 C.F.R. § 603.2(b).

§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

Known as the "Red Flags Rule", § 681.2 requires the development of an Identity Theft Prevention Program (the "Program") designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA). The Program is designed around the concept of "Red Flags", which mean a pattern, practice or specific activity that indicates the possible existence of identity theft. The Program must be designed to first identify the relevant "Red Flags" and risk factors inherent in the User's system; second to establish and administer the Program based on the identified "Red Flags" and risk factors; and third to detect and appropriately respond to Red Flags as they arise. Finally, the Program must be updated periodically as changes are made to the User's systems or as new risk factors are identified.

Other Definitions related to § 681.2:

- Identity theft means fraud committed or attempted while using the identifying information of another person without authority.

- A "covered account" means:

  1. An account that is designed to permit multiple payments or transactions, such as a loan that is billed or payable monthly, and

  2. Any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

- A "creditor" means any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month.

  Note: Although the FTC, in many contexts, does not have jurisdiction over not-for-profit entities, it has taken the position that not-for-profits are subject to FTC jurisdiction when they engage in activities in which a for-profit entity would also engage. In its July 2008 guidance, the FTC stated "Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

§ 681.2 applies to Walla Walla University because of the tuition payment plans offered to our students and student participation in the Perkins, Nursing, and Institutional Loan programs. It also applies to ID Cards issued by Walla Walla University to its faculty, staff and students that can be used to make purchases at various pay points on campus (with the charges added to student or employee accounts which must then be repaid).

§ 681.3 Duties of card issuers regarding changes of address.

Requires that issuers of debit and credit cards notify cardholders of a request to change their own address to the cardholder's former address or by other means mutually previously agreed upon. Does not apply to Walla Walla University as it does not issue debit or credit cards (ID Cards do not meet definition).

II. IDENTITY THEFT PREVENTION PROGRAM

Purpose:

The Identity Theft Prevention Program (the "Program") has been designed to assist Walla Walla University (the "University") in complying with the Federal Trade Commission's (FTC) Identity Theft Rules (16 CFR 681). The Program enables the University to protect new and existing customers, reduce risk from identity fraud, and minimize potential damage to the University from fraudulent new accounts.

Objectives:

1. Assess the existing identity theft risk for new and existing covered accounts;
2. Select measures that may be used to detect risks when they occur in covered accounts;
3. Identify procedures for employees to prevent the establishment of false accounts and procedures for employees to implement if existing accounts are being manipulated;
4. Train the appropriate employees on the Program's policies and procedures; and
5. Update the plan annually with review and approval by the Finance and Facilities Committee of the Board of Directors.

Scope:

This policy and protection program applies to students, employees, contractors, consultants, temporary workers, and other workers at the University.

Policy:

Covered Accounts

a. A covered account is any type of an account or payment plan that involves multiple payments or transactions. This program covers every new and existing account for which there is a reasonably foreseeable risk of identity theft and/or for which there is a reasonably foreseeable risk to the safety or soundness of third parties or to the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

The University has identified the following covered accounts: (1) Student Accounts, (2) Employee Accounts, and (3) Student Loans.

Red Flags – Risk Factors

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

a. The types of covered accounts as noted above;

b. The methods provided to open covered accounts generally include the following:

   1 Student Accounts: Acceptance to the University and enrollment in classes, including a common application with personally identifying information, official high school transcript and official ACT or SAT scores.

   2 Employee Accounts: Submission of employment documents that satisfy I-9 requirements.

3 Student Loans: Submission of loan application, FAFSA application and execution of promissory note.

c. The methods provided to access covered student accounts: See Appendix B.

d. The University's previous history of identity theft.

Red Flags –Identification

The following "Red Flags" are identified and adopted by the Program to detect potential fraud, consumer reports and background checks that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, suspicious documents, suspicious personal identifying information and unusual use of, or suspicious activity related to a covered account. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

1. Fraud or active duty alerts included with consumer reports or background checks;
2. Notice of credit freeze provided by consumer reporting agency;
3. Notice of address discrepancy provided by consumer/background reporting agency;
4. Inconsistent activity patterns indicated by consumer report such as:
    a. Recent and significant increase in volume of inquiries
    b. Unusual number of recent credit applications
    c. A material change in use of credit
    d. Accounts closed for cause or abuse
5. Identification documents appear to be altered;
6. Photo and physical description do not match appearance of applicant;
7. Other information is inconsistent with information provided by applicant;
8. Other information provided by applicant is inconsistent with information on file;
9. Application appears altered or destroyed and reassembled;
10. Personal information provided by applicant does not match other sources of information (e.g. credit reports, social security number not issued or listed as deceased);
11. Lack of correlation between the social security number range and date of birth;
12. Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application);
13. Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager);
14. Applicant fails to provide all information requested;
15. Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet;
16. Identity theft is reported or discovered;
17. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

18. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account;
19. The University is notified by customers, victims of identity theft, law enforcement authorities, or other persons of unauthorized charges or transactions in connection with a customer's covered account;
20. The University is notified that the customer is not receiving paper account statements; or
21. A request made from a non-University issued e-mail account.
22. Unusual use of account; account used in a manner that is not consistent with historical patterns of activity.

Red Flags – Detection

The Program will detect red flags relevant to each type of covered account as follows:

1 Refund of Credit Balances: Refund requests from current students must be made in person by presenting a picture ID or in writing from the student's University issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing picture ID. Requests from students not currently enrolled or graduated from the University must be made in writing. **Red Flags –** Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account. Address requested for mailing refund does not match addresses on file.

2 ID Cards: Charges to student or employee accounts at the various campus pay points must be made in person. **Red Flags –** Picture ID not appearing to be authentic or not matching the appearance of the student or employee presenting it.

3 Student Loans: Requests must be made in person by presenting a picture ID or in writing from the student's University issued e-mail account. The loan check can only be mailed to an address on file or picked up in person by showing picture ID. **Red Flags –** Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account. Address requested for mailing refund does not match addresses on file.

Response to Red Flags:

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the University from damages and loss.

1. Gather all related documentation;
2. Take appropriate action proportional with the degree of risk posed.
3. Write a description of the situation (see Suspicious Activity Report) and send report to Campus Security. Report should include description of Red Flag(s), action taken, outcomes of action taken and assessment of effect, if any, to ongoing Program risk.

If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Monitoring a covered account for evidence of identity theft;

2. Contacting the customer;
3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
4. Reopening a covered account with a new account number
5. Notifying Campus Security and/or law enforcement; or
6. Determining that no response is warranted under the particular circumstances.

Oversight of Program:

Responsibility for developing, implementing and updating this Program lies with the Vice President for Financial Administration who shall be the Program Administrator. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of University's staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for prevention and mitigation of identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program.

Reports to the Board:

The Program Administrator shall at least annually address before the Finance and Facilities Committee of the Board (a) material matters pertaining to the Identity Theft Program, (b) changes in service provider arrangements, (c) effectiveness of the policies and procedures in addressing the risk of identity theft in connection with covered accounts, (d) significant incidents involving identity theft and management's response and (e) any recommendations for material changes to the Program. Issues of material significance will be shared with the Board as deemed appropriate by the Finance and Facilities Committee and the Program Administrator.

Staff Training:

The Chair/Director of each University department with covered accounts (see Appendix A) is responsible to identify red flags and conduct training for all employees, consultants, contractors, temporary workers, and other workers for whom it is reasonably foreseeable that they may contact with accounts or personally identifiable information that may constitute a risk to the University or its customers (see Identity Theft Training Record). To ensure maximum effectiveness, employees may continue to receive additional training as changes to the Program are made. The Risk & Safety Officer will annually communicate with these departments, update the Program as necessary and submit a report to the Program Administrator.

Periodic Update and Review:

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

1. The experiences of the University with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the types of accounts that the University offers or maintains;

5. Changes in the business arrangements of the University.

See assessment of current University Identity Theft Risk as of the date this policy is adopted.

Service Provider Arrangements:

It is the responsibility of the University to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Red Flag Rule and validated by appropriate due diligence, may be considered to be meeting these requirements.

Notices of Address Discrepancy on Consumer Reports and Background Searches:

It is the responsibility of the University to ensure that policies and procedures exist to establish a reasonable belief that a report relates to the consumer about whom the report was requested. Reasonable belief will be established by both Student Financial Services and Human Resources through the maintenance of records that are based on third party documentation (e.g., copy of state driver's license and social security card).

Adopted by the Board of Directors of Walla Walla University on the 1st day of May, 2009.

Updated on April 22, 2024 to include updated Appendix A.

DEPARTMENTS WITH COVERED ACCOUNT INTERACTION [APPENDIX A]

The initial list of departments that have been identified as having interaction with covered accounts is set forth below. These departments will be required to undergo training under the Walla Walla University Identity Theft Prevention Program and will be required to report at least annually to Risk and Safety Management regarding the effectiveness of the Program. As the Program is updated periodically, additional departments may be added to this list.

LIST OF DEPARTMENTS WITH COVERED ACCOUNTS INTERACTION:

		RED FLAGS DETECTION		
		Account Refunds	ID Card Purchases	Student Loans
1	Accounting	x	x	x
2	Student Financial Services	x	x	x
3	Academic Records	x		x
4	Human Resources	x	x	
5	The Express		x	
6	University Bookstore*		x	
7	Sodexo/Cafeteria*		x	
8	Library		x	
9	Technology **		x	
10	ASWWU		x	

* External Service Providers

** Aviation Lessons (Setting up Flight Schedule Pro accounts)

Department List Updated as of 05/13/24

REPORT FROM NANCY CLEVELAND, STUDENT FINANCIAL SERVICES

When a student completes financial clearance the first time, their name and account information is sent to BankMobile so a BankMobile disbursement method can be set up for them. In the mail, the student then receives a letter with information concerning their account and instructions on how to select their disbursement method. A disbursement method is needed in order for them to get disbursements from any credit on their student account. A student can request funds from their student account via an online form found at: http://wallawalla.edu/refund. For security sake, the student must log in using their myWWU user name and password to gain access to the form. They just fill in the amount they wish to have and the date they want the funds. They also have to indicate whether they are a graduate or an undergraduate student. Once they submit the form, it is routed to a financial counselor who approves/denies their request.

Approved requests are processed once a day at 11:00 am. The student's name, ID# and the approved amount is then sent to BankMobile. A wire transfer of actual funds is sent early in the afternoon to BankMobile. Once the wire is received, BankMobile then forwards the funds to the student via the method they selected. They can choose to have the funds transferred to their bank account (the option we highly recommend), have a paper check mailed to them, or have the funds credited to their BankMobile card like a prepaid credit card.

Should a student come in to our office to request a disbursement, we generally have them use one of our computers to complete the Student Credit Balance Refund Form. Students who email counselors asking for funds are sent an email through their WWU email with a link to the online request form.

Updated April 4, 2017

REPORT FROM GEORGE BENNETT
DIRECTOR, CAMPUS SECURITY, WALLA WALLA UNIVERSITY

I have checked back through my 12-year tenure as Director of Campus Security and the only incident that stands out was reported on January 21, 2007. A former student stole her roommate's WWU ID Card and used it at the Express pumps. This ID Card Theft resulted in WWU reimbursing the student's account around $385.00 and WWU was listed in the court documents as a victim and was included in the restitution amount for the perpetrator who was convicted of using a stolen electronic access device.

More recently there was a misuse of some meal cards that Enrollment issued to a prospective student. She did not use all the punches on the cards and gave them to a sibling. The sibling then went to the Express and used them for a $120+ purchase. I talked with the student and had her pay back the amount as the cards were not issued to her and were for "meals" for the visitor. Not hardly an identity theft but of note anyhow.

We have had over the years, stolen WWU ID Cards used at the Café but not for a long while that have been reported to us.

Here are the current ID Card "Points of Use" that could be susceptible to Identity Theft:

1. Access control DSX- system allows cancelation of old card and new card will work. Requires manual entry.
2. Express- does not differentiate between an old card and a new card. May read info but does not use it as of now. I think it could. This would allow the Express to deactivate old cards that may have been stolen.
3. U-Store-system reads all 13 digits but does not use the incremental digit. They would put up notice of stolen card and check the picture.
4. Sodexho-Updates with additions daily in the morning. Have to be told of subtractions and can only flag an account by ID number to check picture id if stolen.
5. Library-Updates once per quarter. It does read the increment digit just after ID number. When new card is used they enter the new info so it will work.

It looks like all the above ID Card Points of Use would need to be notified separately to handle a missing or stolen card. The Express is the most vulnerable due to the ability to swipe at the pump with no employee interaction and no way to flag a particular ID number. However, this vulnerability is mitigated by video monitoring (which is how we caught the perpetrator on January 21, 2007).

Glad you are working on this.

George Bennett
Director, Campus Security
Walla Walla University
204 S College Ave
College Place WA 99324
509-527-2613

Walla Walla University
SEVENTH-DAY ADVENTIST HIGHER EDUCATION

SUSPICIOUS ACTIVITY REPORT

WWU Identity Theft Prevention Program

Reporting individual		Department	

PART I Subject Information

1 Type of covered account a ☐ Refunds b ☐ ID card purchases c ☐ Student loans

2 Individual's last name	3 First name	4 Middle initial

5 Address

6 City	7 State	8 ZIP code	9 Country

10 WWU ID (if applicable)		11 Telephone number

PART II Suspicious Activity Information

12 Date of suspicious activity	13 Total amount involved
	$

14 Detailed description of suspicious activity and red flags detected

15 Actions taken to respond to and mitigate the risk of identity theft (indicate if additional follow-up is required)

a Reported to law enforcement? ☐ Yes ☐ No

Signatures	Date
Reporting Individual	
Campus Security	
Risk & Safety Officer *(Human Resources)*	

Walla Walla University
Identity Theft Training Record

The Chair/Director of each University department with covered accounts (see Appendix A) is responsible to identify red flags and conduct training for all employees, consultants, contractors, temporary workers, and other workers for whom it is reasonably foreseeable that they may contact with accounts or personally identifiable information that may constitute a risk to the University or its customers. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made. The Risk & Safety Officer will annually communicate with these departments, update the Program as necessary and submit a report to the Program Administrator.

Department: _____

Date of Training: _____

Trainer's Name: _____

Type of Training: _____

Name (printed)	**Signature**