

Seattle Pacific University Computer and Information Systems Policies, Procedures, Plans and Standards

Identity Theft Prevention Program and “Red Flags Rule”

Effective: May 1, 2009
Approved by President’s Cabinet on: May 4, 2009

Program and Policy Developed by:
Computer & Information Systems
Student Academic Services
Student Financial Services
University Services
Finance and Budget
Human Resources

Contents:

1.0 Introduction/Purpose

2.0 Definitions

- A. Identity Theft
- B. Red Flags Rule
- C. Red Flags
- D. Covered Accounts
- E. Sensitive Personal Information (SPI)

3.0 Identification and Detecting of Identity Theft Red Flags

Identification of Red Flags

- A. Alerts, notifications or warnings from consumer reporting agencies
- B. Suspicious documents submitted by students or staff
- C. Suspicious personal identifying information submitted by students or staff
- D. Suspicious account activity or unusual use of an account
- E. Alerts from others

Detecting Identity Theft

- A. Verify Identity
- B. Authenticate account holders
- C. Monitor transactions
- D. Verify address changes

4.0 Preventing and Mitigating Identity Theft at SPU

- A. Verification of Identity
- B. Authentication of Students and Employees
- C. Monitor Transactions and Account Activity
- D. Create and Maintain a Secure Online Environment
- E. User Training Program
- F. Office and Department Training Program

5.0 Hard Copy and Electronic Record Protection

- A. Hard copy records
- B. Electronic records
- C. Certain information should not be kept

6.0 Reporting and Responding

- A. Data breach laws
- B. Correct the problem
- C. Assist students and employees
- D. Notification of law enforcement

7.0 Third Party Service Providers

8.0 Identity Theft Program Review and Updates

1.0 Introduction/Purpose

Seattle Pacific has adopted an Identity Theft Prevention Program to establish reasonable policies and procedures to detect, identify, and mitigate instances of identity theft. The Federal Trade Commission (FTC) has issued regulations (the Red Flags Rule) requiring financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions (FACT) Act of

2003. The Red Flags Rule for colleges and universities includes accounts for individuals who defer payments or for whom the University bills for services rendered. The University believes it is a "creditor" under the regulations and therefore subject to the rules.

The University's Identity Theft Prevention Program is intended to:

- Identify the risks for new and existing accounts the University maintains for students and staff
- Detect activities that raise suspicion of fraudulent activity
- Respond to the risks exposed from fraud and identity theft incidents that have been attempted or committed
- Establish guidelines and protocol for periodic review and update of the program.

Several University departments perform activities that are covered under this Identity Theft Prevention program. Working together, these departments have determined the steps that are reasonable and appropriate for the program, and will train the employees in their respective departments to implement these rules.

Computer & Information Systems (CIS) is designated the lead department to coordinate the Identity Theft Prevention program. As the program administrator, CIS will work with the various campus departments to develop and implement these policies and procedures. CIS will convene the primary campus stakeholders as needed to mitigate for fraud and theft under this program.

2.0 Definitions

- A. Identity Theft – a theft by a person or persons of an individual's (or individuals') personally identifiable information for the purpose of opening new accounts, misusing existing accounts, creating fraudulent transactions for goods or services, or accessing other printed or electronic information in order to commit crimes.
- B. Red Flags Rule – the Federal Trade Commission (FTC) and other federal banking agencies, as a part of the Fair and Accurate Credit Transactions (FACT) act of 2003, have issued regulations known as the "Red Flags Rule" which are intended to reduce the risk of identity theft. These regulations apply to financial institutions and creditors holding covered accounts. The rules mandate that a prevention program to protect against identity theft be developed and implemented.
- C. Red Flags – warning signs, patterns, activities, or indicators that might provide opportunities to identify, detect, and prevent identity theft.
- D. Covered Accounts – SPU student and employee accounts include transactions that are defined under "covered accounts" including:
 - Federal Perkins Loan program
 - Other SPU loan programs
 - Tuition payment plans
 - Registration and advance payment plans
 - Meal plans
 - Fines or fees for parking or the library
- E. Sensitive Personal Information (SPI) – there are many data items that, if stolen, could be used fraudulently or to steal. These data elements are identified to require special attention, specifically in regards to identity theft. There are also overlapping policies regarding directory information (as defined under FERPA) that govern the release and handling of some of these data items.
 - Social Security Numbers, Student ID Numbers, Tax ID Numbers, Employee ID Numbers
 - Names, addresses, phone numbers
 - Date of Birth
 - Credit card numbers, expiration dates and PIN's
 - Computer account credentials and passwords
 - Paychecks, pay stubs or other employment records
 - Income tax documents and records
 - Maiden names or parents names
 - Medical information, Insurance information

3.0 Identification and Detecting of Identity Theft Red Flags (derived from FTC FACT Act, Red Flags Rule, Appendix J to Part 681)

Red Flags are signs, patterns, or indicators that might point to suspicious or fraudulent activity. These Red Flags are a starting point for investigation, monitoring, detection, and assessment.

Identification of Red Flags as listed in the guidelines,

- A. Alerts, notifications or warnings from consumer reporting agencies.
- B. Suspicious documents submitted by students or staff.
- C. Suspicious personal identifying information submitted by students or staff.
- D. Suspicious account activity or unusual use of an account.
- E. Alerts from others.

Detecting identity theft should include,

- A. Verifying identity.
- B. Authenticating students and employees.
- C. Monitoring transactions.
- D. Verifying address changes.

4.0 **Preventing and Mitigating Identity Theft at SPU**

Based on the FACT Act and the Red Flags Rule guidelines, SPU has developed the following policies and procedures to prevent and mitigate identity theft. Each department may have a unique set of interactions, transactions, and activities to be performed with students or staff. Proper procedures and training must take place at the departmental level to protect sensitive information, detect the red flags of identity theft, and guard against risks that might arise from that unit.

This policy covers electronic records of people in Banner, Recruitment+, Raiser's Edge, Blackboard, Cbord, and **any other system** that stores sensitive personal information that could be used for identity theft.

This policy also applies to paper and hard copy records that contain sensitive information.

A. Verification of Identity –

- 4.A.1 Review sources of personal identification – watch for documents provided that appear to have been forged or altered, a photograph or physical description that is not consistent with appearance, addresses or names that do not match other records or information on file, documents that appear to have been destroyed and reassembled, documents provided that are not consistent when compared against external information sources.
- 4.A.2 Review official documents – verify names, nicknames or full names that do not match other records, SSN's that are duplicate or do not match information already on file, incomplete addresses or mail drops, incomplete personally identifying information submitted, inability of an account holder to provide authenticating information when asked.
- 4.A.3 New records - when students or employees are added or modified in Banner or other systems (Admissions, Personnel Action Form, Term Contract, Non-Pay Form), as much personally identifying information as possible should be gathered, verified and recorded. This information can be used in later steps to reduce the chance of fraud and increase the detection of suspicious activity.
- 4.A.4 Persons conducting identity verification should ask for both internal identification (SPU Campus Card or ID number) and an additional outside ID that is not already recorded in Banner (Driver's License, other photo ID, passport) for proof of identity.
- 4.A.5 SPU Campus Card issuance – SPU Campus Cards are used for a wide range of identification. When issuing cards the person must already exist in Banner and at least one additional outside picture identification will be provided.
- 4.A.6 Manage release of information – strengthen verification of the identity of people that request information (in person, via phone, via email). Monitor requests for transcripts, statements, or other information for possible fraud.
- 4.A.7 Phone or email inquiries by persons other than the student. Be cautious about parents or spouses that may try to impersonate account holder. SPU staff should use the security questions and information found in ZEIFRPA to verify the identity of the person they are interacting with and only release information as authorized by the student.
- 4.A.8 Review SSN and date-of-birth discrepancies that may be submitted through the Admissions/FAFSA process.
- 4.A.9 Audit for duplicate SSN's in Banner to correct account creation or modification errors.
- 4.A.10 Future/other Items:
 - 4.A.10.1 Scan Driver's License or other photo ID for ongoing identification verification (document imaging system)
 - 4.A.10.2 Capture account holder signatures for further verification and comparison to other documents (document imaging system)
 - 4.A.10.3 Create better account verification questions and answers based on Banner data elements (shared among many departments). Three to five questions to assist in authenticating identity.

B. Authenticate Students and Employees –

- 4.B.1 Require strong authentication methods (across all systems) for students and staff to access and maintain their records and perform transactions.
- 4.B.2 Monitor systems and logs for repeated account lockouts or failed password attempts.
- 4.B.3 Change account credentials, PIN's or passwords if theft or compromise is suspected – if a suspicious activity or Red Flag indicator is presented that points to a reasonable likelihood of compromise, account and user credentials should be modified to block access until use and identification can be verified.
- 4.B.4 Require identity confirmation to perform manual PIN or password resets (that can't be completed through self-service modules).
- 4.B.5 Future/other items:
 - 4.B.5.1 Increase the strength of the Banner credential (tie to domain credential)
 - 4.B.5.2 Strengthen "self service" PIN reset process (security question and answer).
 - 4.B.5.3 Strengthen manual PIN reset process and coordinate between multiple offices (authenticating identity, creating a secure PIN, required change on first login)
 - 4.B.5.4 Provide an email confirmation to account holders for manual PIN resets through self-service systems
 - 4.B.5.5 Audit for frequent manual PIN or password resets, or other significant credential changes and might indicate hacking or other credential abuse.
 - 4.B.5.6 Eliminate SSN as alternate credential (ID number)
 - 4.B.5.7 Eliminate birth date as initial PIN
 - 4.B.5.8 Implement a password change policy (across all systems)
 - 4.B.5.9 Investigate more sophisticated authentication mechanisms (two-factor verification)

C. Monitor Transactions or Account Activity –

- 4.C.1 Departments should develop a matrix of transactions that can be tracked and monitored for Red Flags and other suspicious activity (credential abuse, check refunds, etc..).
- 4.C.2 Verify address changes – address changes are one common area where identity theft can begin. Changing addresses may provide access to other printed material that can be used in theft of information.
 - 4.C.2.1 Match address changes to postal service records (is it a valid address)
 - 4.C.2.2 Monitor returned mail, incomplete address records.
 - 4.C.2.3 Audit for no active mailing address, but ongoing account activity.
 - 4.C.2.4 Skiptrace software centralized use and access (coordinate with Partners)
 - 4.C.2.5 Email confirmation of certain address changes?

- 4.C.3 External partners or reporting agencies may provide fraud or active duty alerts. Request notices of a credit freeze, notices of address discrepancies, a recent increase in volume of inquiries, an unusual number of recent credit relationships, accounts being closed or identified for abuse.
- 4.C.4 Track alerts and notifications from the IRS that an SSN is wrong or a duplicate (student or employee tax information).
- 4.C.5 Monitor credit card charge disputes that may indicate fraud or abuse.
- 4.C.6 Monitor for suspicious account activity – address changes followed by a refund request, rapid increase in activity level or inquiry level, mail sent that is returned multiple times as undeliverable, documents or checks submitted that match other fraudulent activity (bounced checks, etc.), missing statements/invoices or other paper records, unusual cancelling of transactions, personally identifying information that is associated with other fraudulent activities (scams, phishing).
- 4.C.7 Monitor alerts from students or employees reporting their information has been misused (victims), reports from law enforcement about identity theft and fraud, reports from others about suspicious activity pertaining to a student or employee (identity has been stolen and is now being misused).
- 4.C.8 Contact/notify the student or employee to verify activities or transactions – the monitoring of routine transactions to determine unusual use patterns or suspicion of inappropriate activity may require personal contact or notification of the student or employee.
- 4.C.9 Future/other items:
 - 4.C.9.1 Create system level reports to watch for various “red flag” indicators (determined by departments).
 - 4.C.9.2 Develop better techniques to monitor and share suspicious activity between various campus departments to mitigate ID Theft and risks. Provide a “red flag” for accounts that may be suspicious for identity theft or unusual account activity.

D. Create and Maintain a Secure Online Environment

- 4.D.1 Maintain strong control over data – all institutional data should be carefully guarded and controlled. Sensitive Personal Information (SPI) requires ever greater management. Extra safeguards must be in place to not distribute SPI more broadly than required. Keeping SPI data stored centrally is the first step in managing its use.
- 4.D.2 Ensure that campus computers are secure - ensure that office computers are password protected, up-to-date, with virus protection, security firewalls, and strong credentials. Encrypt data stored on desktop and laptop devices to reduce risk of theft or loss. Require secure access to wireless networks.
- 4.D.3 Ensure the SPU websites and other online resources are secure - Ensure that servers, websites and databases are well protected, regularly tested, and up-to-date. Perform regular audits of systems, servers, services, and logs to assure data security.
- 4.D.4 Monitor for suspicious network activity and might indicate keystroke loggers, or other malware used to capture device activity. Network sensors, firewalls, intrusion detection systems and reports.
- 4.D.5 Lock down compromised accounts and require password resets and user notification in the event of suspicious account activity or release/communication of credentials.
- 4.D.6 Regularly audit desktop, laptop, and server security procedures and policies to assure a high level of protection is in place. Perform penetration testing to confirm security of resources.
- 4.D.7 Future/other items:
 - 4.D.7.1 Limit access to the SSN field in Banner
 - 4.D.7.2 Automate permission creation and maintenance based on attributes stored in Banner that govern access
 - 4.D.7.3 Adopt more advanced tools to detect system or security compromises, software malware and rootkits, and other hacking attempts.

E. User Training Program

- 4.E.1 Provide appropriate policies, procedures and standards to document best practices for data security, identity theft tricks and techniques, emerging tools to reduce the risk and mitigate the occurrences of fraud and misuse. Publish guidelines and procedures as appropriate.
- 4.E.2 Create a culture or awareness and knowledge about ID theft, and the procedures in place to mitigate the risk.
- 4.E.3 Train campus students and employees regarding data security, phishing scams, virus and malware protection, and other social engineering compromises.
- 4.E.4 Require FERPA training for all employees that have regular access to academic records (to include academic records in addition to the SPI data that could be used for ID Theft).
- 4.E.5 Continue October Security Awareness Month (including ID Theft and FERPA awareness)
- 4.E.6 Encourage students and employees to request copies of credit reports at least once a year.
- 4.E.7 Future/other items:
 - 4.E.7.1 Annual FERPA “refresher” for all employees that access academic records
 - 4.E.7.2 Develop a departmental level security training program for staff
 - 4.E.7.3 Create an online user security training program

F. Office and Department Training Program

- 4.F.1 Provide appropriate policies, procedures and standards to inform departmental employees regarding ID Theft and the indicators outlined under this policy. Publish guidelines and procedures as appropriate.
- 4.F.2 Continue April Data Security Awareness Month (data management policies, system protections, awareness)
- 4.F.3 Require VPN training for all employees provided off-campus access to secure centralized resources.
- 4.F.4 Future/other items:
 - 4.F.4.1 Create an online departmental security training program
 - 4.F.4.2 Post reminders in areas where sensitive information is stored and used.

5.0 Hard Copy and Electronic Record Protection

All University employees must take steps to protect sensitive personal information they may have access to or collect from students and staff. The following policies and procedures should be followed.

A. Hard copy records

- 5.A.1 File cabinets, desk drawers, or other storage locations that contain documents with sensitive information will be locked and secured when not in use.
- 5.A.2 Paper documents containing sensitive information will not be left on desks, tables, work areas, printers, fax machines, or other non-secure locations.

- 5.A.3 Documents containing sensitive information will not be stored longer than is needed and will be securely destroyed and discarded when no longer needed.
- 5.A.4 Identified paper/hard copy records to be reviewed
 - 5.A.4.1 Income Tax returns stored for Financial Aid processing
 - 5.A.4.2 Paper Registration and Student files (registration, internships, others.)
 - 5.A.4.3 Employee forms that contain SPI data
- B. Electronic records
 - 5.B.1 Electronic records that contain SPI data shall be stored and maintained on central servers. Whether the record is in a database form, an email message, a word or excel document – the most effective method to protect the data is to know where it is stored.
 - 5.B.2 While email is a convenient messaging tool, please **AVOID** transmitting confidential or sensitive personal information through email. Messages can be potentially intercepted as they travel across the internet, and once data is transmitted via email the opportunity to contain the distribution is lost.
 - 5.B.3 Employees that create, store or manage documents and worksheets on campus provided computers (desktops or laptops) shall keep those documents within their "Documents" folder tree so that they are stored centrally and encrypted on the local device.
 - 5.B.4 SPI data shall not be stored on portable media (CD's, DVD's, USB drives, or removable hard disk drives).
 - 5.B.5 SPI data (and most other campus/employee data for that matter) shall not be stored on home computers or personally owned mobile devices.
- C. Certain information should not be kept
 - 5.C.1 Compliance with Payment Card Industry-Data Security Standards (PCI-DSS) requires that credit card transactions not be stored within on-campus databases or on local servers that have not passed external audit controls. For SPU, this means that a third party payment processor will be used for all online transactions that process credit card payments.

6.0 Reporting and Responding

The policies and procedures outlined in this document are intended to reduce the disclosure of data that can be used for identity theft. Detecting activities where theft may have occurred will require an appropriate response to the potential risk.

SPU will respond in a reasonable and timely manner to possible data breaches and indicators of ID theft.

- A. Data breach laws – most states (currently 44 states) have laws dealing with the accidental disclosure of SPI data. The State of Washington, RCW 19.255.010, dictates that we must disclose any breach of system security to state residents whose unencrypted personal data was, or is reasonably believed to have been, acquired by an unauthorized person. Personal data (for data breach purposes) in Washington is defined as:
 - First name or initial and last name in combination with any of the following data elements,
 - Social Security Number (SSN)
 - Driver's License number or state issued ID card
 - Account number or credit card number, in combination with security code, access code, or password that would permit access to an individual's financial account
- B. Correct the problem – following this policy may identify activities or procedures where the risk of ID theft can be reduced or mitigated. In those cases -- reasonable and timely correction, reporting, implementation, analysis, and review will be conducted.
- C. Assist students and employees – in addition to preventing, detecting and mitigating instances of ID theft, the university may at times assist students and employees that may have been victims and had their credit history damaged.
- D. Notification of Law Enforcement – in the event that we have determined actual fraud or theft to have taken place, we will notify the appropriate law enforcement agencies as required.

7.0 Third Party Service Providers

The obligations to detect, prevent and mitigate instances of identity theft are passed on to university vendors who are performing duties as the university or on behalf of the university. In circumstances where SPI data has been provided to third party vendors, those vendors must provide a written Identity Theft Prevention Program with Red Flag components.

Whenever SPU engages a third party or service to perform an activity that may include or expose SPI data, the university will review that the policies and procedures of the vendor are reasonable to detect, prevent and mitigate the risk of ID theft.

Current known vendors:

- A. Campus partners for student loan data
- B. Collection Agencies (past due student accounts)
- C. Third Party Credit Card Processors (NetNet/InfiNet)
- D. Cbord (ID Card, meal plan Vendor)
- E. National Student Clearinghouse
- F. Vuetura Package Tracking

8.0 Identity Theft Program Review and Updates

The Identity Theft Prevention program will be reviewed and updated on a periodic basis as changes in risks, potential red flags, means of detection, and analysis of incidents, takes place.

The policy implementers and approvers will be kept apprised on a periodic basis of changes to the policy and significant incidents.