September 21, 2017

18-050 ADOPT THE INITIAL IDENTITY THEFT PREVENTION PROGRAM DOCUMENT AS REQUIRED UNDER 16 C.F.R. PART 681 (RED FLAGS RULE)

PREPARED BY: Dee Wilson, Bursar and Treasury Manager, Financial Services

APPROVED BY: Eric Blumenthal, Associate Vice President, Finance
Jim Langstraat, Vice President, Finance and Administration
Mark Mitsui, College President

REPORT: In November, 2008, The Federal Trade Commission issued a regulation known as the "Red Flags Rule," (16 C.F.R. Part 681) requiring financial institutions and creditors that hold certain covered accounts to develop and maintain a written identity theft prevention program that detects and responds to red flags for identity theft.

In April, 2009, the Portland Community College Board enacted Policy B 710 - Identity Theft Prevention Program. At that time, an initial Program document was created but not formally adopted as required by the federal regulation. § 681.1(b)(3) requires the institution to:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

The Program document originally created in 2009 was recently updated to reflect the current administration and structure of the Program.

RECOMMENDATION: That the Board of Portland Community College:

1. Approve the "PCC Identity Theft Prevention Program" document in Exhibit B
2. Directs that the President assign a program administrator with responsibility for overseeing, communicating, administering, and maintaining the identity theft prevention program; for training staff as necessary to effectively

implement the program; and for exercising appropriate and effective oversight of any service provider arrangements performing any services for the College relative to covered accounts as required under the Red Flag Rule.

PCC IDENTITY THEFT PREVENTION PROGRAM

I. Purpose

Portland Community College (PCC or the College) developed this Identity Theft Prevention Program (Program) pursuant to the Federal Trade Commission's (FTC) Red Flags Rule. The Red Flags Rule implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The College's Identity Theft Prevention Program (Program) is designed to detect, prevent, and mitigate identity theft in connection with the opening and maintenance of covered accounts for students and employees.

The Program, authorized under Board Policy B710, defines processes and procedures to guide employees in departments involved with covered accounts in identifying and responding to patterns, practices, or specific activities (Red Flags) that indicate the possible existence of identity theft.

II. Definitions

A. Covered account:
   1. All student accounts or loans administered by the College, including tuition payment plans, federal and schools loans.

   2. Other records the college offers or maintains where payment is accepted or credit is extended and there is a reasonably foreseeable risk of identity theft to the person or a risk to the safety and soundness of the college's records including financial, operational, compliance, reputation or litigation risks.

B. Identifying information**:** Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, bank account number, student identification number, or credit or debit card number.

C. Identify theft**:** A fraud committed or attempted using the identifying information of another person without authority.

D. Program Administrator: The individual designated with primary responsibility for oversight of the Identity Theft Prevention Program.

E. Red Flag: A pattern, practice or specific activity that indicates the possible existence of identity theft.

III. Program

A. The college hereby establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program includes procedures to:

1. Identify red flags for covered records and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any detected red flags to prevent and mitigate identity theft; and
4. Update the Program periodically to reflect changes in risks to students or employees and to ensure the safety and soundness of the college from identity theft.

IV. Program Administration

The associate vice president of financial services shall serve as the Program Administrator.

A. The Program Administrator is responsible for:

1. Obtaining approval of the initial written Program from the College's Board of Directors;
2. Implementing the Identity Theft Prevention Program;
3. Conducting periodic reviews of compliance with the Program;
4. Ensuring compliance with the Program's training requirements;
5. Approving material changes to the Program as necessary to address changing identity theft risk

B. The Program Administrator shall:

1. Review and update this Program at least once a year to reflect changes in regulatory requirements and risks associated with covered accounts;
2. Consider the college's experience with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the college's business arrangements with other entities;
3. Assign appropriate personnel to serve on a Red Flag Incident Review Team (RFIT) and Red Flag Oversight Committee (Committee);
4. Make necessary updates to the Program;
5. Notify the college president of any substantive changes to the Program or risks to the College.

V. Departmental Compliance:

A. Deans, directors, and heads of departments that work with covered accounts are responsible for:
   1. Conducting a risk assessment to determine areas of vulnerability for identity theft within their operations;
   2. Implementing departmental processes for complying with this policy;
   3. Ensuring that employees responsible for compliance attend required training.

B. Employees of departments that work with covered accounts shall:
   1. Attend training provided by or under the direction of the Program Administrator in the detection of Red Flags and the steps to be taken when a Red Flag is detected;
   2. Comply with the Program and notify the Program Administrator of identified failure to comply with the Program;
   3. Identify relevant Red Flags appropriate for their operations;
   4. Implement departmental policies and procedures to detect and prevent Red Flags and respond appropriately to mitigate identity theft;
   5. Report potential Red Flags and any suspicious behavior that may be related to identity theft.

VI. Identifying Red Flags

In order to identify red flags, the college considers the types of records it maintains, the methods it uses to open and access records, and its previous experiences with identity theft. Red Flags generally fall within one of the following four categories: suspicious documents, suspicious personal identifying information, suspicious or unusual use of accounts, and/or alerts from others (e.g. customer, identity theft victim, or law enforcement). Examples of Red Flags include, but are not limited to, documents that appear to be forged or altered, conflicting demographic information, mail returned as "undeliverable" although transactions continue on the account, or a notice or inquiry from a fraud investigator.

VII. Detecting Red Flags

A. New Records: In order to detect any of the red flags identified above associated with a new record or which presents a foreseeable risk of identity theft, college personnel will obtain and verify the identity of the person opening the account and review documentation for Red Flags or independently contact the student or employee.

B. Existing Records: In order to detect any of the Red Flags identified above for an existing record, personnel will take steps to monitor transactions, such as verifying identity when information is requested; verifying the validity of address change

requests, and verifying changes in banking information given for the purpose of payments. College personnel have the discretion to determine the degree of risk posed and to act accordingly.

VIII. Preventing and Mitigating Identity Theft

In order to further prevent the likelihood of identity theft, College personnel will take appropriate steps, commensurate with the degree of risk posed, regarding ongoing internal operating procedures. College personnel have the discretion to determine the degree of risk posed and to act accordingly.

IX. Reports

The Red Flag Incident Response Team (RFIT) shall review all Identity Theft received to ensure appropriate action is taken to mitigate risk and prevent future instances. Members of the RFIT shall prepare a semi-annual Red Flag Report for the Program Administrator. The report shall address the effectiveness of the policies and procedures related to the opening and maintenance of covered accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

X. Program Updates

The Committee will periodically review and update the Program to reflect changes in risks to students and the soundness of the College from Identity Theft. In doing so, the Committee will consider the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

XI. Service Provider Arrangements

In the event the college engages a service provider to perform an activity in connection with a covered account, the college will take the following steps to ensure the service provider performs in accordance with the Program:

A. Require, by contract, that service providers have appropriate policies and procedures in place designed to detect, prevent, and mitigate identity theft; or

B. Require, by contract, that service providers review this Program and report any red flags to the Program Administrator; and

C. Require that contracts include indemnification provisions limiting the college's liability for the service provider's failure to detect, prevent, or mitigate identity theft.

XII. Non-disclosure of Specific Practices

A. Disclosure of specific information or practices regarding red flag identification, detection, mitigation and prevention practices may be limited to designated college staff and/or policymakers. Documents produced to develop or implement the Program which describe specific practices may constitute security information and may be non-disclosable because disclosure would likely jeopardize the security of identifying information and may circumvent the college's identity theft prevention efforts.

B. Non-disclosure of Specific Practices: For the effectiveness of the Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation, and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential and should not be shared with other College employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

XIII. DATE OF APPROVAL: