COLORADO
COMMUNITY COLLEGE SYSTEM

Annual FACTA Report

Prepared as part of the System's Response to the Fair and Accurate Credit Transactions Act of 2003

July 2021

Submitted by Michael A. Schulman

Director of Student Affairs

Landon K. Pirius, Ph.D.

Vice Chancellor for Academic and Student Affairs

Table of Contents

CONTENTS

Introduction 3
Arapahoe Community College 5
Community College of Aurora 7
Community College of Denver 9
Colorado Northwestern Community College 13
Front Range Community College 15
Lamar Community College 18
Morgan Community College 20
Northeastern Junior College 22
Otero Junior College 23
Pueblo Community College 25
Pikes Peak Community College 30
Red Rocks Community College 32
Trinidad State Junior College 34
CCCOnline 37
Appendix I 39
- REFERENCES: 39
- PROGRAM STATEMENT 39
- SCOPE 39
- BACKGROUND 39
- DEFINITIONS 40
- IDENTIFICATION OF RED FLAGS 40
- DETECTING RED FLAGS 41
- RESPONSES TO RED FLAGS 41
- Protect Student Identifying Information 43
- PROGRAM ADMINISTRATION 43

Appendix II 46
- Purpose 46
- What is a Red Flag? 46

College Responsibility 47
Current Practices that Prevent, Detect and Mitigate Identity Theft 47
ENROLLMENT 47
EXISTING ACCOUNTS 48
FORMS OF CONTACT 48
FINANCIAL AID 50
ADDITIONAL PROCESSES FOR FINANCIAL AID 50
Appendix III 53
NEW CONTRACT LANGUAGE: 53

INTRODUCTION

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) was passed by Congress to protect consumers from inaccurate credit information and credit fraud. The law is best known for providing consumers with the opportunity to receive on an annual basis a free credit report.

Higher education institutions are covered under the law because its involvement with tuition payment plans and student loans. Also, some colleges provide information to consumer reporting agencies, which is also a covered action under the act. This means that colleges and universities must adopt and follow a written identify theft policy. For the Colorado Community College System, that policy is BP 4-60, and the procedure related to the policy is SP 4-60. The system also adopted an Identity Theft Prevention and Detection program and Identity Theft and Mitigation Business Process. Together, these written documents detail how students must verify their identification to receive services, ways in which to reduce the chance of identity theft, what to do if someone makes a complaint of identity theft or if identity theft is suspected, and an annual evaluation of the program.

Each college is required to have a program coordinator and there is a system administrator at the system office.

System activities undertaken, in part to improve the processes included:

- In conjunction with a cyber security consultant and legal counsel, a new System Procedure is being developed to clearly define how colleges can share data internally via e-mail and shred drives, as well as how data can be shared with extremal partners who are allowed to receive information under FERPA including but not limited to benefit provides, Colorado Department of Higher Education, and the National Student Clearinghouse.
- The communication plan previously established and shared with the Financial Aid Directors for reporting financial aid fraud has been updated to include additional types of fraud.

These policies cover all thirteen colleges and the system office. While the system office does not have students, because the system provides on-line courses and has a help desk that assists in resolving issues with student's on-line issues, it was reviewed as well.

For the annual evaluation, the colleges were asked to respond to the following questions:

- The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

- The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

- The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

- Please list any significant incidents involving identity theft within the college and management's response to those incidents.

- Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

Based on the written reports, it appears that the System's policies and procedures are effective. Despite a substantial turnover of program coordinators, the training and on-boarding was handled well by the colleges.

Colleges reported that annual and on-going training exists for new and current employees so that student transactions and records are properly conducted and protected.

All third party service providers have agreements that protect student records.

Ideas for improving the identify theft prevention program include:

- Offer a system-wide template, similar to FERPA that could be sent internally to make all staff and faculty aware of FACTA.
- Provide updated training for Program Coordinators on an annual basis.

This report will be shared with senior administrators at the system office and colleges as well as the program coordinators.

The following sections include the college reports as well as the system policies and procedures.

Colorado Community College System
Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Arapahoe Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

The policies and procedures addressing the risk of identity theft in connection with student services transactions are effective. Policies and Procedures exist related to verification of student identity for student service transactions and new staff are trained on these policies and procedures directly by their Supervisor as they are hired. Additionally, periodic refresher trainings are held for existing staff prior to the start of each larger semester.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

The policies and procedures addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts are effective.

- As students apply for admission, they are asked to provide personal information (beyond the basics of Birth Date, Address, etc.) that is the kind of information usually only known to the student.
- Each student has a unique Student Identification Number assigned to them at the time of application, and they create a personalized password and answers to security questions for use when accessing their student account.
- In compliance with SP4-60, student identity is verified in Student Services transactions by either the student producing a secure and verifiable document, a college or high school identification card, or answering a series of questions unique to the student.
- Email communication regarding student education record information is done only to / from two college-assigned, college-controlled email addresses (e.g. Faculty institution email to student CCCS email; Faculty institution email to Staff institution email; student CCCS email to Staff institutional email, etc.).
- Minimal documents containing student personally identifiable information are printed, and only when absolutely necessary, then are immediately placed in a secure shred receptacle when no longer needed.

- Student-use computers are monitored and if any student is finished using the computer, but has inadvertently left it logged in to their account, staff log-off for the student.
- Applications for admission received by the institution are scrutinized when certain data elements seem suspicious (e.g. multiple applications submitted with the same DOB and same address but different names). In these instances, holds are placed on the student accounts seeking additional documentation to verify the identity of the student.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

The policies and procedures addressing the risk of identity theft in connection with service provider agreements are effective. All contracts with service providers include the requirement that the service provider comply with all federal and state laws, and that they have taken appropriate steps to comply with the Fair and Accurate Credit Transactions Act of 2003.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

None

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

Expand the measures to ensure student identity when accessing their online course(s).

Colorado Community College System
Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2018-2019

Community College of Aurora

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

Current business processes and guidelines are very effective in protecting student information.

All new employees in the departments of Financial Aid, Fiscal Services and Enrollment Services are provided FERPA training and additional training is provided employees in these departments at regular staff meetings as needed.

The Community College of Aurora "Notification of Rights under FERPA" is posted on the CCA website.

As part of new employee orientation, the human resources department reviews with the new employee the following: 1) CCA's Student Records/FERPA policy. 2) Verification of Identity. The new employee then signs a cover sheet indicating review of the information.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

Community College of Aurora adheres to the following guidelines:

- FERPA guidelines
- BP 4-60 State Board for Community Colleges and Occupational Education Acceptable Identification Process for Student Services Transactions
- Colorado Community College System President's Procedure Acceptable Identification Process for Student Services Transactions
- Colorado Community College System Educational Services Council Guidelines Directory Information

The policies and procedures provide valuable guidance used to protect student accounts. We believe our policies and procedure are quite effective in mitigating the chances of identity theft occurring on campus.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

Service provider agreements must abide by our FERPA requirements, therefore no information about a person's account may be released by or to a service provider without signed permission by the covered account owner. Requests from third party(s) for information about an account must have a signed release by the account holder indicating precisely what information the account holder is having the College release to the requestor.

Student Loan Clearinghouse and Higher One have many security measures in place that reflect the requirements of FERPA and FACTA.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

There are no known cases of identity theft during the year. No reports have been filed with law enforcement by students claiming identity theft and no subpoenas have been received for open investigations relating to identity theft.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

Community College of Aurora has no recommendations at this time.

Colorado Community College System
Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Community College of Denver

Per the Colorado Community College System's Identify Theft Prevention and Detection Program (Program), the College program coordinator is required to submit an annual report to the System program administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

Community College of Denver (CCD) effectively meets the requirements of the Program in regards to student transactions by following the processes outlined in the Identity Theft and Mitigation Business Process. Identity verification following SP 4-60 policy is consistently practiced at Registration and Records, Advising, Student Life, Testing, TRiO, Cashier's Office, Tutoring, Resource Center and Financial Aid Customer Service counters. During New Student Orientation, student identity verification is confirmed during the check-in process.

In New Employee Orientation, FERPA and the student verification process are covered in addition to System President's General Computer and Information Systems Procedures (SP 3-125), which lists steps College employees must take to maintain the confidentiality of data and prevent unauthorized access to information system.

The College communicates internally regarding FACTA and FERPA requirements by sending an annual college-wide e-mail to notify College employees of FACTA requirements (sent out by Human Resources) and FERPA requirements (sent out by Office of Registration and Records).

The College communicates externally and to students by publishing information about FACTA in the Catalog each academic year and sending out an Annual FERPA Notification, which notifies students of their rights afforded under FERPA. The FERPA notification is also published in the Catalog each academic year. CCD publishes relevant student rights and FERPA/FACTA information on the College website in the online catalog as well.

FERPA and other legal notices are covered during New Student Orientation and are available to all students.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

Community College of Denver effectively meets the requirements of the Program in regards to the opening and maintenance of Covered Accounts by adhering to the guidance provided by CCCS System President's Procedure (SP 4-60) and SBCCOE Board Policy (BP 4-60) to prevent unauthorized disclosure of education records under FERPA and to protect Personally Identifiable Information (PII) of Covered Accounts. When accessing Covered Accounts, College staff and student/work study staff are trained to obtain an I.D. as proof of identity and/or use of security questions to confirm student identity. If a student is unable to provide this information, no student **record** information will be given. In all forms of contact, which includes telephone and email inquiries, students are required to verify their identity by stating their student number and answering security questions. When communicating with students on-line regarding PII or education record information on Covered Accounts staff will only do so through the student's system-assigned e-mail account.

CCD's Financial Aid Department adheres to the CCCS Potential or Substantiated Financial Aid Discrepancy Business Process by utilizing its authority to resolve conflicting information. Staff members are trained to detect unusual commonalties between multiple FAFSAs and verification documents. If a staff member becomes aware that a student is submitting information already tied to another student's record, they will select the student for verification group 4. Verification group 4 requires proof of identity, high school completion and educational intent. In situations that require escalation, the Financial Aid Director will utilize the Financial Aid Discrepancy holds as appropriate, notify CCCS Legal and proper CCD/CCCS personnel, as well has make a referral to the U.S. Department of Education's Office of Inspector General.

CCD employees, full-time and part-time, professional and student/work study employees are currently being trained in the procedures to follow in responding to Immigrations and Customs Enforcement (ICE), Department of Homeland Security (DHS), the Auraria Police and other law enforcement requests to disclose PII information on Covered Accounts according to CCCS guidelines. Academic Centers, Enrollment, and Student Services Centers collaborate with the Student Conduct Office as well as the Auraria Police Department in reporting, addressing and resolving fraudulent activities.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

Community College of Denver effectively meets the requirements of the Program in regards to service provider agreements by including a FERPA statement in every third-party agreement and strict adherence to FERPA requirements for all third-party requests/collaborations and requires the student's written consent prior to the sharing of any educational records. Student information between Metropolitan State University of Denver (MSU Denver) and University of Colorado Denver (CU Denver) is conducted through secure and encrypted exchange.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

Date	Incident
8/5/2020	CCD Foundation received an email notification from Blackbaud (3rd party scholarship application provider) that a ransomware attack was launched against their platform. No student data or donor data was breached.
8/7/2020	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
8/7/2020	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
8/17/2020	FA employee accidentally shared 4,052 personal email addresses to the same 4,052 former CCD students. There were 2 batches. One batch sent to 3,755 and one batch sent to 297 people. She emailed an informational ECMC flyer the aforementioned population with the subject line "**IMPORTANT** Re: Defaulted student loans? We got a solution!". Instead of using the "BCC" option to mask the email addresses, she used the "TO" option. FA Director became aware of the incident on the following Monday when a complaint was forwarded to her from the Student Conduct Office. FA director notified Department of Ed and all appropriate CCD and CCCS staff as required by the Security Incident Reporting Form. An email was also sent to all affected students.
9/3/2020	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
9/4/2020	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
9/18/2020	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
10/30/2020	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
12/2/2020	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
1/8/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
1/25/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
2/10/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
2/23/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]

3/18/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
3/25/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
4/29/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]
6/2/2021	The Debt Management and Collection Services center for Maximus Federal contacted Financial Aid Director T Lavin for documentation pertaining to [redacted]
6/17/2021	T Lavin sent 62 student IDs to the Office of Inspector General regarding a suspected financial aid fraud ring. It is believed that up to 500 2020-2021 may be fraudulent. CCCS legal and all CCD and CCCS appropriate personnel were notified.
6/29/2021	The Fraud and Identity Theft Department of Nelnet contacted Financial Aid Director T Lavin for documentation pertaining to an identity theft claim made by former student borrower [redacted]

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

CCD had plans to create a fraud prevention/identity theft mitigation taskforce, however priorities and resources had to be shifted as a result of COVID-19. As operations return to campus the creation of the taskforce is under reconsideration. Members of the committee will include representatives from the Financial Aid Office; Office of Registration and Records; Admissions Recruitment and Outreach; the Testing Center; and Instruction

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Colorado Northwestern Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

Policies and procedures packets are provided to all new employees at the time of hire. The packets include FERPA and SP 4-60 of which is gone over with each new employee in detail. While new employees are trained for the job these policies and procedures are reviewed and put into practice during on the job training by supervisors. Ongoing training on these policies is provided yearly at convocation and can be referenced in the convocation handbooks, our website, and the CCCS website. CNCC struggles to have a transparent process about how to report identity theft concerns and with the turnover of the Vice President of Student Services in February 2021, plans mentioned in the 2019-2020 FACTA report for delegating this to a specific student services department did not occur.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

Policies and procedures for opening and maintenance of Covered Accounts require proof of identity followed as stated in SP 4-60 and FERPA regulations. Supervisors monitor employees to ensure the procedure is followed.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

Service providers understand and adhere to identity theft policies and procedures. National Student Clearinghouse and BankMobile have many security measures in place that reflect the requirements of FACTA.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

One incident was reported to Kelly Scott, Interim Vice President of Student Services.

Date	Incident
6/2/2021	SS# for a student is off by one number. The social security number we have on file is incorrect. A non student with that SSN had her income tax refund withheld because the student who'd incorrectly applied with her SSN has been sent to collections. The person with the SSN number on file will be filing this information with the State of Colorado in order to have her income taxes reinstated back from us to her. Non-student contacted law enforcement to file a report.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

The need for increased awareness of the need to report any concerns about identity theft was discussed at a 6/30/21 Student Services departmental meeting. It was decided to report any concerns identified by staff or stakeholders through the incident/complaint form. By submitting the issue this way, we can be certain it is tracked, shared with the appropriate people and resolved. A follow-up email reminding staff of the board policy and the new process was sent on 6/30/21. This process will be even more important as the VPSS role will transition again and we want to ensure some continuity. A formal training on how to handle different identity theft incidents for the FACTA Coordinator would help the next VPSS.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Front Range Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

- As part of their onboarding process, all new employees at Front Range Community College are required to review and acknowledge internal FRCC organizational guidelines. These guidelines cover many areas that relate to the FACTA requirements.
- Employees also complete an online FERPA tutorial. The results are sent to their supervisor and the Registrar. This tutorial includes questions related to protecting student records and data security.
- In order to receive computer access, new employees must sign a Security and Confidentiality Agreement. This agreement covers user's responsibilities, right and restrictions surrounding use of college computers and systems.
- We utilize a Clean Desk Policy which includes users locking their PC when stepping away, clearing desk off every night of any personally identifiable information (PII) and securing PII in locked cabinet.
- Financial Aid has an additional new employee orientation since their access to student records includes sensitive information due to the nature of Financial Aid data. New employee orientation includes review of two separate checklists:
  - The administrative checklist includes items such as review of Code of Ethics, Financial Aid Office Standards of Excellence and Institutional and Department Guidelines and Procedures
    - Additionally, employees must review and complete the FSA Coach Modules and quizzes by passing with an 80% or higher. Certificates are provided to the FA Training & Compliance Officer to maintain on file
    - All new employees are also required to go through the NASFAA Core training which consists of 13 modules and a toll kit to introduces federal student aid programs

- The Fiscal department uses a training plan for new employees that includes responsibilities with system access request/limits; informing them of office procedures. These procedures include secure workspace training, locking computers, and the duty to ensure that faculty/student secure information is protected. Access to the Cashier's Office is strictly limited.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

- College service areas follow the proof of identity procedures as outlined in SP 4-60, Acceptable Identification Process for Student Services Transactions. Procedures are posted in service areas for quick reference.
- Strict adherence to the Family Education Rights and Privacy Act (FERPA). In the case of a FERPA violation, students are given the option to request a new Student ID number and to mark their record confidential.
- New employees are required to read and sign the Computer Use policy SP3-125c and are required to read the Data Security, FRCC internal guideline IS-8.15.
- Access to the Student Information System (Banner) is restricted by role and function, to limit access to student records.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

The majority of service provider agreements are contracted by CCCS and therefore monitored by CCCS.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

Financial Aid is currently working on or has concluded work on several cases in the past year. These were requests related to federal student aid from outside agencies where are required to provide documentation/data.

- U.S. Department of Education Office of Inspector General; suspected fraud cases (CCCS was apprised)
- Mohela Loan Servicer; student claiming identity theft and/or suspected fraud
- Navient Loan Servicer; students claiming identity theft and/or suspected fraud
- Nelnet Loan Servicer; students claiming identity theft and/or suspected fraud

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

- Updated training for Program Coordinators.

- FACTA Coordinators could come together to create a system wide email template that could be sent internally to make all staff and faculty aware of FACTA, similar to the FERPA notice that is sent to students, staff and faculty.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Lamar Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

The policies and procedures addressing the risk of identity theft in connection with student services transactions are effective. Our Human Resources Department has created a checklist for all new employees to speak with individuals on campus about specific policies and procedures. New employees are directed to the FACTA College Program Coordinator to discuss the Identity Theft Prevention and Detection Program. Procedures exist related to verification of student identity for student service transactions and new staff team members are trained on these policies and procedures directly by their supervisor as they are hired. Additionally, periodic refresher trainings are held for existing staff prior to the start of each fall and spring semester.

New employees are trained to understand that they must follow the CCCS procedures on verifying identity in-person and on the telephone. We use a rule of three: the individual must be able to identify three pieces of information that are not easily known.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

The policies and procedures addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts are effective. Lamar Community College adheres to the following guidelines:

- FERPA guidelines
- BP 4-60 State Board for Community Colleges and Occupational Education Acceptable Identification Process for Student Services Transactions
- Colorado Community College System President's Procedure Acceptable Identification Process for Student Services Transactions
- Colorado Community College System Educational Services Council Guidelines Directory Information

- Access to the Student Information System (Banner) is restricted by role and function, in order to limit access to student records.

The policies and procedures provide valuable guidance used to protect student accounts. The Financial Aid Office, Cashier's Office and the Admissions Office are all included in these processes. All of these offices flag suspicious applications or documentation from the time students initially apply.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

The policies and procedures addressing the risk of identity theft in connection with service provider agreements are effective. All contracts with service providers include the requirement that the service provider comply with all federal and state laws, and that they have taken appropriate steps to comply with the Fair and Accurate Credit Transactions Act of 2003. We require a signed authorization by the student before any information would be released to any third party.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

None – By implementing the CCCS process mentioned above and flagging potential fraud applicants, we did not have any identity theft issues during the 2020-2021 year.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

Continue annual training for FACTA Program Administrators and Coordinators.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Morgan Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

The current policies and procedures are effective in the protection of student's personally identifiable information (PII) data. As part of the new employee orientation checklist they must attend an in-person FERPA training where we talk about protecting everyone's identity and whom to report issues to. MCC staff also talk about the release form that students can complete telling us who and what information can be released. MCC reviews this each academic year with front line staff and reminds them the release requires an annual request.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

MCC has implemented the CCCS Policy for Potential or Substantiated Financial Aid Discrepancy Business Process. The Financial Aid, Admission's, Cashier, and the Student Services Offices are all included in this process. All of these offices flag suspicious applications for documentation from the time they initially apply. MCC has implemented the use of BDM at our centers to send information back and forth (image documents such as tax forms, etc.) so that we do not fax personal data.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

The Student Loan Clearinghouse and BankMobile (formerly Higher One), Maxient, and Follett have many security measures in place that reflect the requirements of FACTA. MCC also requires a signed authorization by the student before any information is released to any third- party (i.e. Voc. Rehab, Social Services, etc.).

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

MCC did not experience any identity theft 2020-2021 year so no remediation was needed.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

MCC continues to post signs notifying all students that they may be asked for proof of identity when making in person transactions with student services, bookstore/cashier, and accounting services. MCC continues to look at ways to limit the transmission of student PII by using internal networks and data retrieval rather than emails.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Northeastern Junior College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

New employees are trained to understand that they must follow the CCCS procedures on verifying identity in-person and on the telephone. We use a rule of three: the individual must be able to identify three pieces of information that are not easily known.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

We have implemented the CCCS Policy for Potential or Substantiated Financial Aid Discrepancy Business Process. The Financial Aid Office, Cashier's Office and the Admissions Office are all included in this process. All of these offices flag suspicious applications or documentation from the time they initially apply.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

We would require a signed authorization by the student before any information would be released to any 3rd party.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

Through the implementation of the CCCS process mentioned above and flagging potential fraud applicants, we did not have any identity theft issues during the 2020-21 year.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

None at this time.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Otero Junior College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

New employees involved in the Student Services area at Otero Junior College attend an orientation in-service training that includes a review of FERPA provisions with emphasis on protecting student identity from any unauthorized use. We follow certain procedures such as issuing picture identification cards for all students and staff. All staff requests proof of identity before any transactions are entered into on behalf of students. We believe our procedures for ensuring protection of identity are effective and work well.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

Otero Junior College has not had any incidences of identity theft in connection with the opening and maintenance of Covered Accounts. We believe our policies and procedures are quite effective in mitigating the chances of identity theft occurring as a result of action and/or inaction on the part of Otero Junior College Employees.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

Service provider agreements must abide by our FERPA requirements therefore no information about a person's account may be released by or to a service provider without signed permission by the covered account owner. Requests from third party(s) for information about an account must have a signed release by the account holder indicating precisely what information the account holder is having the College release to the requestor.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

Otero Junior College has had no incidents involving identity theft of any significance.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

Otero Junior College has no recommendations at this time.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

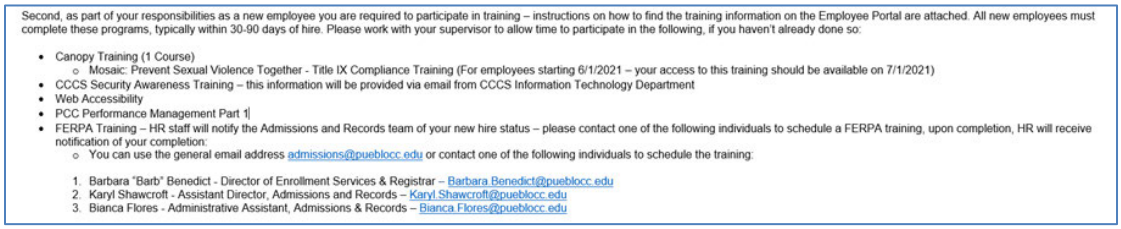
Pueblo Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

The business processes and guidelines that directly relate to the protection of PII during student services transactions are effective and adequately communicated to PCC's new hires.

- The New Employee Orientation specifically addresses FERPA training. From the orientation email sent to new hires:



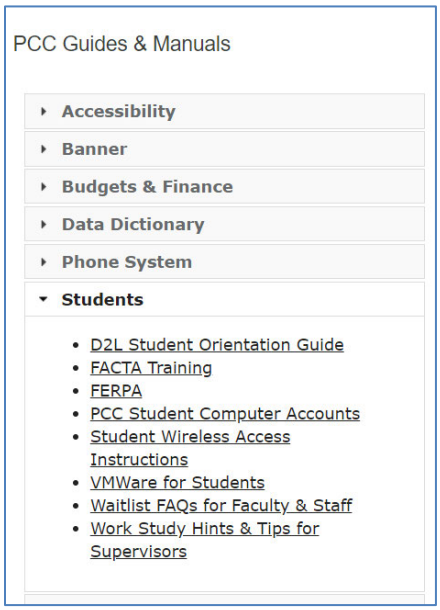
Second, as part of your responsibilities as a new employee you are required to participate in training – instructions on how to find the training information on the Employee Portal are attached. All new employees must complete these programs, typically within 30-90 days of hire. Please work with your supervisor to allow time to participate in the following, if you haven't already done so:

- Canopy Training (1 Course)
  - Mosaic: Prevent Sexual Violence Together - Title IX Compliance Training (For employees starting 6/1/2021 – your access to this training should be available on 7/1/2021)
- CCCS Security Awareness Training – this information will be provided via email from CCCS Information Technology Department
- Web Accessibility
- PCC Performance Management Part 1
- FERPA Training – HR staff will notify the Admissions and Records team of your new hire status – please contact one of the following individuals to schedule a FERPA training, upon completion, HR will receive notification of your completion:
  - You can use the general email address admissions@pueblocc.edu or contact one of the following individuals to schedule the training:

1. Barbara "Barb" Benedict - Director of Enrollment Services & Registrar – Barbara.Benedict@pueblocc.edu
2. Karyl Shawcroft - Assistant Director, Admissions and Records – Karyl.Shawcroft@pueblocc.edu
3. Bianca Flores - Administrative Assistant, Admissions & Records – Bianca.Flores@pueblocc.edu

- Prior to being granted network access, all new hires are required to sign a "Security and Confidentiality Agreement," which describes the user's restrictions and responsibilities regarding the use of State-owned equipment.
- New student workers receive detailed training related to the area in which they are employed and must sign off on their receipt and understanding of detailed FERPA/identity verification business process documents; additionally, returning student workers are required to attend annual training sessions that reinforce the tenets of FERPA and the verification of identity for student services transactions processes.
- As the COVID-19 crisis required that the majority of student services transaction be conducted remotely, PCC's *Operating Protocol S-307 Verification of Identity for Student Services Transactions*, which defines directory information, lists the "secure and verifiable documents" required for verification of identity, and details the specific procedures required prior to release of PII, was reviewed and instructions for video conferencing was added and distributed to staff and faculty.
- The Director of Financial Aid presented training to student services and academic personnel on the requirements of Gramm-Leach-Bliley, the responsibilities to secure student financial data, and the reporting obligations should a data breach occur.

- Student identity theft training materials are available to new instructors in the Adjunctorium, D2L's faculty training component.
- Internal communication of FACTA and FERPA requirements is accomplished through the annual email notification to PCC employees from HR (FACTA) and Admissions and Records (FERPA).
- The Director of Financial Aid and the Registrar developed a FACTA training presentation that is available to employees through their myPCC Portal accounts on the Resources, Training, and Tools tab (below). This training is presented to new hires in conjunction with their required FERPA training.



The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

Regarding the maintenance of student accounts, PCC complies with the requirements of FERPA; CCCS' "Business Processes for the Identification and Mitigation of Identity Theft'; SBCCOE BP 4-60 "Acceptable Identification Process for Student Services Transactions"; PCC Operating Protocol S-307 "Verification of Identity for Student Services Transactions; and CCCS' President's Procedure SP 4-80a "Student Educational Records and Directory Information".

- During the application process, PCC admissions operators follow the procedures specified in CCCS' "Admission Application Process" document, which require the use of common matching rules that compare applicants' information against data already captured in the System schools. Applications with discrepancies or potential conflicts in vital information are suspended for further investigation. These same matching rules are utilized during the FAFSA load process.
- PCC adheres to the CCCS "Incorrect Identity/Potentially Fraudulent Record" business process when managing records that may be associated with identity theft issues. With application and the creation of "covered accounts," PCC protects the identity of

the account owners and limits access to the information contained in these accounts in all student services transactions. Protections include:

- PCC's new Director of Institutional Research is currently reviewing the content of the daily strategic planning reports sent to members of the PCC community to ensure that the recipients have the legitimate academic interest necessary for access to the information.
- Both the MyPCC Portal and Navigate login requires both username and password, and students who forget either their SID or password are required to use the "Student Identity Tool," which presents the student with a set of identity verification questions that can change as students' enrollment progresses;
- Correction of mismatched data can only occur with visual inspection of identification (SSN card and valid ID);
- Student-use computers are overseen and monitored by PCC staff and student workers. When students use the computers, the workstations are immediately inspected upon the student finishing to ensure that proper logout has occurred and no printed materials are left at the workstation.
- Any email communication involving student educational records is performed only among and through college-assigned and -controlled email addresses (NAME@student.cccs.edu; NAME@pueblocc.edu, or NAME@ucourses.com).
- For phone conversations, identity is verified through the use of specific and consistent questions as noted in PCC Operating Protocol S-307 "Verification of Identity for Student Services Transactions" with the understanding that only very limited information can be discussed by phone;
- PCC staff protect student information by locking workstation screens when upon leaving the line of sight, by disposing of documents in compliance with Colorado records retention schedules, and by locking storage units that house hard copy documents that may potentially contain PII;
- All enrollment records kept by the PCC VA Desk in order to facilitate the correct certification of enrollment for VA educational benefits that were previously maintained in hard copy files have been moved fully online to an access-protected database;

- All in-person student services transactions require that the student provide proof of identity through a secure and verifiable document as described in SP 4-60, examples of which may include:
  - PCC Panther Pride student ID card/high school ID card;
  - Valid state-issued driver's license or ID card;
  - Valid passport with photo;
  - Military ID;
  - Certification of Naturalization/Citizenship with photo;
- Students must provide written consent prior to the institution's disclosure of PII/education records. PCC's term-specific "Student Records Release Form" requires that the student identify what information will be released, the purpose of the release, and to whom the information will be released. The person listed on the form as the recipient of the information must provide proof of identity before any sensitive information is released. For AY2020-2021, PCC had two records release forms, one durable Power of Attorney form, and one proof of

conservatorship on file. One student asked that a previously requested confidentiality hold be maintained for the duration of AY20-21.

- Access to Banner and Cognos is restricted by role and function as determined by the requesting staff's supervisor and upon approval of the PCC Registrar.
- Mobile Record Shredders maintains secure bins in multiple campus sites in which paper documents slated for destruction are placed. Individual office suites contain portable shredders for use in destroying documents that may contain PII but need not be preserved and retained as part of official business. Financial Aid view/modify Banner permissions have been removed from general security profiles and have been restricted to those roles that explicitly require access to student financial data.
- Access to BDM has been implemented at all PCC campuses and sites in order to eliminate the need to email/fax PII.
- PCC's Office of Financial Aid complies with the CCCS "Potential or Substantiated Financial Aid Discrepancy" business process by resolving conflicting information immediately upon discovery. Staff review documents for incongruities. Discrepancies among family members may result in another family member's selection in Verification Group 1 (requires submission of tax return transcripts and W2 forms), and, when fraud is suspected, that student is selected in Verification Group 5 (requires proof of identity and high school completion and statement of educational intent).

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

Primary service providers include the Student Loan Clearinghouse/NSLDS (enrollment and degree verification), BankMobile (refund processing services), Maxient (behavior records), CASHNet, ECMC Group (student loan guaranty agency) and EAB (the Navigate student engagement and enrollment management platforms).

- The Clearinghouse and NSLDS utilize U.S. Federal encryption standard protocols to collect, maintain, and distribute sensitive information.

- BankMobile utilizes Oracle Fusion Middleware software solutions, which ensures that all online data transmissions between PCC and BankMobile are encrypted.

- Maxient's Shibboleth/SAML2 is a version of the Security Assertion Markup Language standard for exchanging authentication and authorization data between security domains.

- CASHNet abides by the security of the Payment Card Industry Data Security Standards (PCIDSS).

- Banner data is FTP'd to Navigate and Campus through the standard network protocols of the client-server model architecture using separate control and date connections between the client and the server.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

PCC had no significant verifiable incidents involving identity theft within the college during AY20-21.

- Records was contacted by one student who reported that she received a bill for classes in which she never enrolled; she was adamant that someone stole her identity. Upon investigation, it was determined that the registration occurred online through the student's MyPCC Portal account. In discussion with the Registrar, the student stated that she had been "playing around" in the Portal at about the time the registration occurred, but didn't think that she had actually enrolled in anything, since she never saw an "Are you sure you want to enroll?" message appear.
- Two instances occurred in which PCC staff members did not pay close enough attention to emails they were sending, and Outlook's autocomplete function filled in the "To" field with addresses similar to the intended recipient. No PII was disclosed in the inadvertent emails, and PCC Communications distributed a tutorial on disabling autocomplete and clearing the autocomplete cache.
- A Help Deck ticket was submitted from a PCC student who noted that MS Azure had not properly been closed and he was able to see student names. The PCC-IT and CCCS-IT Help Desks investigated the issue; the PCC-IT Help Desk reported to the Registrar that no records were compromised.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

None at this time.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Pikes Peak Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

PPCC Enrollment Services uses a rotating set of questions when complying with SP 4-60.

At this time, all new employees must attend an orientation which includes red flag indicators of possible identity theft. Employees are trained on FERPA and given procedures and processes on SSN changes, name changes, identification requirements in all scenarios to include in person, on the phone, and through student assigned email.

Employees are trained to be sensitive to the surroundings in each area. Some of these things include inside voices, front areas (no sensitive materials visible during work hours), back-end processors (lock up sensitive information every night), computers are always locked when leaving the desk, and keeping all shredding in the locked shred bins.

Ongoing/refresher training is also conducted. Student Services holds professional development days on every Friday morning from 8 a.m. to 9 a.m. in which trainings take place.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

All covered accounts can only be accessed by the person on the account, or a person or agency identified by the account holder. The account holder may sign a FERPA Consent Form allowing another access to the account. The form must be completely filled out and signature must be witnessed by a staff person from the institution, or the signature must be notarized.

The only account information given out is the directory information listed in our catalog. An account holder may request no information be given out by signing a request to keep records confidential.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

Service provider agreements must abide by our FERPA requirements; therefore, no information about a person's account may be released by or to a service provider without signed permission. If a third-party requests information about an account, they must have a signed release from the account holder.

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

The only big thing PPCC has still had ongoing is the Financial Aid Fraud which has affected all colleges within our system. All departments are on high alert and inform Financial Aid and the Registrar if an account looks questionable. A hold is placed on the account and if documentation and identity cannot be confirmed, the information is forwarded to the CCCS legal department.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

I would like to see another training about FACTA. It has been a very long time since there have been any trainings. To train staff at our college, we should also be given annual trainings to stay up to date with the process.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Red Rocks Community College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

Each department is responsible for training new employees on FERPA. I have been asked to attend department meetings throughout the year to provide an overview of FERPA. I also will meet with new hires at the request of the supervisor for individual FERPA training.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

Red Rocks Community College follows the following guidelines:

- FERPA guidelines
- State Board for Community Colleges and Occupational Education BP 4-60 Acceptable Identification Process for Student Services Transactions
- Colorado Community College System President's Procedure Acceptable Identification Process for Student Services Transactions
- Colorado Community College System Educational Services Council Guidelines Directory Information

New accounts that appear to be duplicated are reviewed. If necessary a registration hold is put on the new account and the student is notified that more documentation is needed.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

N/A

Please list any significant incidents involving identity theft within the college and management's response to those incidents.

I am not aware of any identity theft incidents during the last academic year.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

N/A

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

Trinidad State Junior College

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

All new employees at Trinidad State College are trained in FERPA policies through an online tutorial regarding directory information and FERPA release forms. New employees are provided with an employment packet concerning acceptable identification process for students, list of random questions to be used to verify the identity of a person on the phone, and requirements of visual proof of identification when data is mismatched in the system, whether it is a SSN, state ID, or other valid ID.

Additional follow up for correct use of FERPA information is completed with the individual supervisors.

Internal communication of FACTA and FERPA requirements is accomplished through the annual email notification to Trinidad State employees from the Registrar's office. The College communicates externally to students by publishing information about FACTA and FERPA in the catalog each academic year and sending out an annual FERPA notification, which notifies students of their rights afforded under FERPA. Trinidad State College publishes relevant student rights and FERPA/FACTA information on the College website in the online catalog as well.

As a service for TSC employees, Trinidad State contracted with a private vendor, Legal Shield, who was available to the employees for consultation and information regarding identity theft.

The institution believes the preliminary trainings, follow up, and consultations have increased the college's effectiveness in regards to reducing the risk of any type of identity theft.

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

Regarding the maintenance of student accounts, Trinidad State College complies with the requirements of FERPA; Business Processes for the Identification and Mitigation of Identity Theft; SBCCOE BP 4-60 “Acceptable Identification Process for Student Services Transactions”; CCCS’ Educational Services Council Guidelines for Directory Information; and CCCS’ President’s Procedure SP 4-60 “Acceptable Identification Process for Student Services Transactions”.

During the application process, TSC admissions operators follow the procedures specified in CCCS’ “Admission Application Process” document, which require the use of common matching rules that compare applicants’ information against data already captured in the System schools. Applications with discrepancies or potential conflicts in vital information are suspended for further investigation. These same matching rules are utilized during the FAFSA load process.

TSC adheres to the CCCS “Incorrect Identity/Potentially Fraudulent Record” business process when managing records that may be associated with identity theft issues.

Trinidad State employees are on the lookout for the red flags of identity theft that may occur in our day to day operations. Red Flags are suspicious patterns of practices, or specific activities that indicate the possibility of identity theft. Some examples include fraud or active duty alert on a credit report, suspicious documents, identification that looks altered or forged, or inconsistencies with what the student has submitted to staff. For instance, an address, phone number, or other personal information already used on an account known to be fraudulent.

The standard business policy for Trinidad State is to protect sensitive information by locking computer screens when walking away from the desk, shredding documents according to the records retention schedule, locking file cabinets and storage rooms containing sensitive information, and locking office doors. Employees are also required to protect documents that are visible on a desk whenever they leave their office or building at the close of the day.

In order to protect individual’s accounts from identity theft, college employees and work studies are required to ascertain acceptable proof of identity before providing information regarding a student’s account. TSC’s policy is to correctly identify a student face to face or via a phone call before giving out any information.

Document scanning has increased protection of student information within a uniform system. Scanned documents are also purged in accordance to the CCCS retention schedule.

When a red flag is spotted, an appropriate response may include some of the following:

- Change passwords, security codes, close an existing account, notify law enforcement.

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

Trinidad State College complies with system policies, and we follow the SP3-125 Computer form that is signed by all new employees of the college.

If students use their own computers/phones they are not protected by the CCCS firewall. It is recommended that they have an updated anti-virus and a firewall for protection.

The Student Loan Clearinghouse and BankMobile (formerly Higher One), and Maxient, have many security measures in place that reflect the requirements of FACTA. We also require a signed authorization by the student before any information is released to any 3rd party (i.e. Voc. Rehab, Social Services, etc.)

Additional services provided for Trinidad State Students are loan entrance counseling, exit counseling, and a “Student Aid and Identity Theft” flyer.

The compliance which co-exists with these companies has been effective in reducing the risk of identity theft for TSJC Students.

Please list any significant incidents involving identity theft within the college and management’s response to those incidents.

During the 2020-2021 school year, there were 95 reports involving identity theft at either our Trinidad or Alamosa campuses. These were reported to our Human Resources department. An e-mail was sent out to staff and students with guidelines informing what response the individual should take. These steps included submitting a fraud report with the Labor & Employment Bureau, filing an online police report, and placing a freeze at the three consumer credit bureaus.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

TSC catalog and website continue to share with staff and students a written Identity Theft Prevention Program that is designed to detect the warning signs – or red flags – of identity theft in our day-to-day operation.

Colorado Community College System

Identity Theft Prevention and Detection Program Annual Report
Due June 30 Each Year
Academic Year: 2020-2021

CCCOnline

Per the Colorado Community College System's Identify Theft Prevention and Detection Program, the college Program Coordinator is required to submit an annual report to the System Program Administrator no later than June 30th of each year. Please address each of the following:

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with student services transactions. Please include how training for new employees is handled.

FACTA policies and procedures are shared with new employees. CCCOnline provides support to all CCCS colleges. We respond to college inquiries regarding possible fraud by providing information available about students enrolled in CCCOnline courses, including course access dates and course activity in D2L.

When a college makes a request about student online course activity, CCCOnline's Academic Technology team checks IP addresses for similar patterns and reports any findings to the CCCOnline Dean of Student Affairs, who sends the information to the colleges

The effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts.

N/A

The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with service provider agreements.

N/A

Please list any significant incidents involving identity theft within the college, and management's response to those incidents.

Summer 2021 semester: Two of CCConline's Department Chairs noticed unusual lack of course participation in their courses. A very high percentage of students in these classes had not logged on or participated the first week of class. Our Student Affairs department reviewed enrollments and discovered odd enrollment patterns by a group of CCD students.

CCCOnline's Manager of Enrollment & Student Success contacted the CCD Registrar, who investigated this, along with the CCD Financial Aid Director, who discovered a "fraud ring" of students, who were dropped from the courses.

Please provide your recommendations, if any, for changes to the program either from a college or System perspective.

None

APPENDIX I

Colorado Community College System

Identity Theft Prevention and Detection Program

REFERENCES:

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

PROGRAM STATEMENT

In accordance with the Fair and Accurate Credit Transactions Act (FACTA) of 2003, this Identity Theft Prevention and Detection Program is intended to prevent, detect and mitigate identity theft in connection with establishing new covered accounts or an existing covered account held by the Colorado Community College System (System or CCCS) or one of its thirteen (13) community colleges, and to provide for continued administration of the Program.

SCOPE

This Program applies to CCCS and its thirteen (13) community colleges.

BACKGROUND

The Federal Trade Commission's (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, requires the establishment and implementation of an Identity Theft Program. The System's Program was developed with oversight and approval of the State Board for Community Colleges and Occupational Education (SBCCOE).

This Program was developed with consideration of the size and complexity of the System's operations and accounting systems, and the nature and scope of the System's activities.

DEFINITIONS

Board – The State Board for Community Colleges and Occupational Education (SBCCOE).

Identity Theft – Fraud committed or attempted using the identifying information of another person without authority.

Authorized Person – Any person whom a student has authorized in writing to obtain information regarding their account.

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

Covered Account – Includes all student accounts or loans that are administered by the System and/or a System College.

Program Administrator – The individual designated with primary responsibility for oversight of the Program.

Institution – Any one or all of the community colleges that are within the System.

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, or student identification number.

IDENTIFICATION OF RED FLAGS

Accounts offered or maintained are primarily receivable accounts that allow students to pay tuition and related charges in installments or defer payment until financial aid is received. Accounts are opened on-line or in-person. Account information is accessible on-line, via telephone or in-person.

The following are considered Red Flags for the purposes of this Program:

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. Suspicious requests for information from individuals other than an authorized person and/or failure to establish identity utilizing System President's Procedure (SP) 4-60, Acceptable Identification Process for Student Services Transactions;
4. Suspicious requests for login information after repeated unsuccessful attempts to login and/or failure to establish identity utilizing System President's Procedure (SP) 4-60, Acceptable Identification Process for Student Services Transactions;
5. A request to mail something to an address not listed on file, with the exception of information that is requested by the student or by an authorized person; and
6. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

DETECTING RED FLAGS

A. Student Enrollment
Student identity will be established during the enrollment as outlined in System President's Procedure (SP) 4-60, Acceptable Identification Process for Student Services Transactions.

B. Existing Accounts
In order to protect student identities of covered accounts, the System and/or System Colleges will verify identification before any action is taken pursuant to SP 4-60, "Acceptable Identification Process for Student Services Transactions."

RESPONSES TO RED FLAGS

In the event that Red Flags are identified, one or more of the following steps should be taken, depending on the degree of risk posed by the Red Flag:

- In the application for admissions process if staff becomes aware that a student is submitting information already tied to another student's record they will notify the applicant of the need to present visual proof of identity using valid identity documents before the application is processed.

- If staff member believes they have been presented with fraudulent identity documents, they will request additional proof of identity and/or additional documentation from the student or prospective student.
- Staff who receive suspicious requests for information from individuals other than an authorized person (per FERPA regulations) will immediately refer the request to the appropriate college staff person or administrator for further review.
- Multiple failed log-in attempts to the student self-service student information account will result in the account being locked and require the student to contact a staff person for assistance.

- Each college must notify consumers through an annual notification and information/link in their catalog and in the portal of their rights under FACTA, steps that consumers can take to protect themselves against identity theft, and college contact information for reporting identity theft concerns.

- Each college must designate a college Program Coordinator (PC) and notify the CCCS Program Administrator of the designation.

- If a staff member has been contacted regarding possible identity theft, the staff member needs to confirm the alleged victim's identity. Once identity has been confirmed, the staff member places a privacy hold on the student's account, gives the students identity theft information, and reports the situation to their direct supervisor immediately. The college will assign the student a new student identification number and transfer all student data/history, place the privacy setting on the new account if student desires, place a Red Flag Hold on the original student account in question, and begin a Red Flag investigation by the designated college official.

- If a staff member has been contacted regarding possible identity theft, the staff member needs to confirm the alleged victim's identity. If staff member cannot confirm identity through normal means and has reason to believe that identity is in question, the staff member needs to notify their direct supervisor immediately and a Red Flag investigation by the college will commence.

- If the Red Flag investigation results in fraud, a Red Flag Hold will be placed on the student's account, and the supervisor will report the situation to the college disciplinary officer for follow-up as appropriate and to the College Program Coordinator for preventing identity theft.

- If situation is deemed to affect another student on campus, that student will be notified of concerns and given information about protecting their identity, including his/her right to a Privacy notice on their student account, creation of a new student account, etc.

- In all cases, the supervisor reviews the information/situation and notifies the College Program Coordinator within 3 working days.

- The College Program Coordinator will review the situation, contact all affected parties, give identity theft prevention information including option to notify local

police, and add information to a standard tracking grid for reporting purposes. All reported situations will be tracked in this manner. The College Program Coordinator will inform CCCS Legal and CCCS Student Affairs apprised of any unusual patterns of activity regarding identity theft issues.

- If Financial Aid (FA) is involved, the Director of Financial Aid will utilize the FA and FD holds as appropriate, notify CCCS Legal and in conjunction with CCCS Legal, make appropriate referral to the Inspector General's Office, U.S. Department of Education.

Protect Student Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the following steps will be taken with respect to internal operating procedures to protect student identifying information:

1. Ensure each College and the System's websites are secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to covered account information are password protected;
4. Limit the use of social security numbers;
5. Ensure computer virus protection is up-to-date; and
6. Require and retain only information that is necessary to conduct official business.

PROGRAM ADMINISTRATION

Oversight

Responsibility for developing, implementing and updating this Program lies with the System Vice President for Organizational Effectiveness, Student Affairs, and Strategic Initiatives who has been designated as the Program Administrator. The Program Administrator will be responsible for ensuring the implementation and continuation of the Program, and maintenance of this document, and for obtaining approval from the Board or designated sub-committee for any changes to the Program.

Each College shall have a Program Coordinator who is responsible for coordinating efforts at their institution. The Program Coordinator will be responsible for identifying appropriate training of staff, reviewing staff reports regarding the detection of Red Flags, ensuring staff follow the steps for preventing and mitigating identity theft and for determining which steps of prevention and mitigation should be taken in particular circumstances. The Program Coordinator will be responsible for certifying to the Program Administrator annually their institution is in compliance with Program requirements.

Staff Training and Reports

College and System personnel shall be trained, as necessary, to effectively implement the Program. College employees are required to notify their Program Coordinator once they become aware of an incident of identity theft or of the institution's failure to comply with any requirement of this Program.

At least annually or as otherwise requested by the Program Administrator, the College Program Coordinator, who is responsible for development, implementation, and administration of the Program at the college level, shall report to the Program Administrator in writing indicating compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with 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.

Service Provider Arrangements

When contracting with service providers who perform services related to covered accounts, the System and all Colleges shall require within the contract or purchase order that the service provider assert their compliance with all federal and state laws, and certify that they have taken appropriate steps to comply with the Fair and Accurate Credit Transactions Act of 2003.

Non-Disclosure of Specific Practices

For the effectiveness of this Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to those responsible for developing this Program and 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 employees or the public, notwithstanding any legal requirements that might require disclosure.

Program Updates

The Program Administrator will periodically review and update this Program to reflect changes in risks to students from identity theft. In doing so, the Program Administrator will consider the System and Colleges' experiences with identity theft, changes in identity theft methods and detection, prevention methods, and changes in System and College 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.

APPENDIX II

Colorado Community College System

Business Processes for the Identification and Mitigation of Identity Theft

(Documented and developed in response to the CCCS Identity Theft Prevention and Detection Program)

Purpose

In accordance with the Fair and Accurate Credit Transactions Act of 2003 (FACTA) and the CCCS Identity Theft Prevention and Detection Program (the Program), these business processes are intended to document how system colleges currently prevent, detect and mitigate identity theft in connection with establishing new covered accounts or an existing covered account held by the CCCS office or one of the state system community colleges, and to provide for continued administration of the Program. In addition, these business processes outline potential future technical and other enhancements to further augment the ability to detect Red Flags as identified in the Program.

What is a Red Flag?

As defined by the Program in accordance with FACTA, a Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

The following are considered Red Flags as defined by the Program and for the purposes of the business processes:

1. Documents provided for identification appear to have been altered or forged;

2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;

3. Suspicious requests for information from individuals other than an authorized person and/or failure to establish identity utilizing System President's Procedure (SP) 4-60, "Acceptable Identification Process for Student Services Transactions";

4. Suspicious requests for login information after repeated unsuccessful attempts to login and/or failure to establish identity utilizing SP 4-60, “Acceptable Identification Process for Student Services Transactions”;

5. A request to mail something to an address not listed on file, with the exception of information that is requested by the student or by an authorized person; and

6. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

College Responsibility

Under Program Administration there is a requirement that each college have a Program Coordinator. Responsibilities are outlined in the Program document under Program Administration and include, but are not limited to:

At least annually or as otherwise requested by the Program Administrator, college staff responsible for development, implementation and administration of the Program shall report to the Program Administrator in writing indicating compliance with this program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider agreements, significant incidents involving identity theft and management’s response, and recommendations for changes to the program

Current Practices that Prevent, Detect and Mitigate Identity Theft

Procedures in college service areas should be reviewed on at least a biannual basis to determine that current practices meet the requirements of the Program.

Services areas include, but are not limited to: Admissions, Records, Registration, Advising, Student Life, Testing, Recruiting, TRIO, Cashiering, Tutoring, TRIO, and Financial Aid. The review should ensure that areas conduct procedures that establish student identity whenever contact is made with a student that involves information on the student’s record.

ENROLLMENT

During the enrollment process, student identity will be established through:

- Proof of identity as outlined in SP 4-60, Acceptable Identification Process for Student Services Transactions

EXISTING ACCOUNTS

In order to protect the identities of the owners of existing accounts, enrollment services staff will follow the processes below in conjunction with the student information system security settings:

- Proof of identity as outlined in SP 4-60, Acceptable Identification Process for Student Services Transactions
- Use of random questions generated by data in the Student Information System to verify the identity of a person on the phone (not sufficient to be DOB and SSN or student ID)
- Strict adherence to the Family Education Rights and Privacy Act (FERPA)
- Requiring visual proof of identification when data is mismatched in the system (across colleges), often including but not limited to, SSN card and state ID or other valid ID
- Require release of information form as needed per FERPA
- Require a student ID and password to access the student information system
- Use of security questions when a student attempts to access his or her password or unique student ID online
- Use of SSN when possible for the online application person matching process (Currently this is the process, but it will be modified shortly due to new ASSET legislation & CE processes)
- Use of common matching rules in the online application process which compares an applicant's information against already existing students system wide. If a potential conflict exists on key information submitted (e.g., DOB and SSN), then the application for admission is suspended for manual review
- Use of common matching rules in the financial aid application load process
- Protect sensitive information by locking computer screens when walking away from desk, shredding documents according to the records retention schedule, locking file cabinets and storage rooms containing sensitive information, and locking office doors
- All departments – develop, adopt, and train valid telephone and email identity procedures for all staff who deal with student information, including work study students in accordance with SP 4-60, Acceptable Identification Process for Student Services Transactions
- All colleges adopt and post language on steps for reporting possible identity theft to include, but not limited to, the Student Information System, college catalog, college portal, and/or college web pages.

FORMS OF CONTACT

For each student services transaction, students are required to verify his or her identity as stipulated in and SP 4-60, Acceptable Identification Process for Student Services Transactions or most student services transactions, with exception to testing services and issuance of a college identification card, a student can verify his or her identification through one of the following:

1. A series of questions unique to that particular student;
2. Producing a college identification card;
3. Producing a high school identification card; or
4. Producing some other form of identification that is considered a "secure and verifiable document" which means it must be issued by a state or federal jurisdiction or recognized by the United State government and that it is verifiable by federal or state law enforcement, intelligence, or homeland security agencies.

If the student is inquiring via the telephone:

- Staff will ask for student number(S#)
- Staff will also ask random questions generated by data in the Student Information System and student must be able to answer 3 questions correctly to verify the identity of a person on the phone as per SP 4-60, "Acceptable Identification Process for Student Services Transactions"
- General information that is not specific to a student can be given out

If the student is inquiring via email:

- As a primary means, staff will respond to college assigned email account
- Colleges may respond to non-college assigned email accounts only if identity has been verified in accordance with SP 4-60, "Acceptable Identification Process for Student Services Transactions"
- General information that is not specific to a student can be sent to any email account

Information being requested by someone other than the student:

- Strict adherence to FERPA (Family Education and Rights and Privacy Act) guidelines is followed by all staff members
- The college FERPA release form must be on file or the FERPA signature must be present on the requesting document (including, but not limited to, transcript requests, letter or recommendation requests)
- The college FERPA release form must be witnessed by a staff member and student's identity must have been verified as noted or the college FERPA release form must be notarized (if received by mail or if being submitted by someone other than the student) or
- The form must also be specific in detail to include dates and specific information requested
- A copy of the request for information will be placed in the Imaging System under the student's S#

- Third Party identification will be made using a photo ID or by the Third Party password created by the student as part of the records release process

Additionally, staff will also protect information by adherence to the following guidelines:

- If a request to mail Personally Identifiable Information or information protected by FERPA to an address not listed on file, with the exception of official transcript requests that are requested by an authorized person; staff will follow protocols for proof of identity and/or ask student to update their official mailing address as appropriate
- Protect all sensitive information by adhering to Board Policy (BP) 3-125, "Electronic Communication Policy," locking computer screens when walking away from desk, using privacy screen for the computers, shredding documents according to the records retention schedule, locking file cabinets and storage rooms containing sensitive information, and locking office doors
- All staff will be strongly encouraged to also adhere to a "clean desk policy" whenever they leave the building at the close of the workday

FINANCIAL AID

If a student applies for Federal financial assistance, student identity will be established through:

- U.S. Department of Education automated processes that verify name, Social Security Number (SSN), and date of birth (DOB)
- If the student is requesting Financial Aid Records information, staff will ask for an acceptable photo ID per SP 4-60, "Acceptable Identification Process for Student Services Transactions," to identify the student

ADDITIONAL PROCESSES FOR FINANCIAL AID

Processes for the Identification and Mitigation of Identity Theft for Financial Aid:

Financial Aid performs procedures that establish student identity whenever contact is made with a student that involves information on the student's record, except when communicating to the college issued email account.

In order to protect the identities of the owners of existing accounts, financial aid staff will follow all of the processes as outlined above for enrollment services staff and the following additional process:

- If a student calls and states that he/she has received financial aid information but has never applied for financial aid, staff will direct the student to speak with the college Director of Financial Aid. The college Director of Financial Aid will gather information from the student, notify CCCS Legal and CCCS Student Services and will contact the Office of Inspector General as appropriate. The college Director

of Financial Aid will also give the student information about his/her rights regarding identity protection.

The business process used for monitoring the occurrence of a Red Flag, the steps to report those occurrences to authorities, and the steps taken to address the occurrence.

- In the application for admissions process if staff becomes aware that a student is submitting information already tied to another student's record they will notify the applicant of the need to present visual proof of identity using valid identity documents before the application is processed.
- If staff member believes they have been presented with fraudulent identity documents, they will request additional proof of identity and/or additional documentation from the student or prospective student.
- Staff who receive suspicious requests for information from individuals other than an authorized person (per FERPA regulations) will immediately refer the request to the appropriate college staff person or administrator for further review.
- Multiple failed log-in attempts to the student self-service student information account will result in the account being locked and require the student to contact a staff person for assistance.
- Each college must notify consumers through an annual notification and information/link in their catalog and in the portal of their rights under FACTA, steps that consumers can take to protect themselves against identity theft, and college contact information for reporting identity theft concerns.
- Each college must designate a college Program Coordinator (PC) and notify the CCCS Program Administrator of the designation.
- If a staff member has been contacted regarding possible identity theft, the staff member needs to confirm the alleged victim's identity. Once identity has been confirmed, the staff member places a privacy hold on the student's account, gives the students identity theft information, and reports the situation to their direct supervisor immediately. The college will assign the student a new student identification number and transfer all student data/history, place the privacy setting on the new account if student desires, place a Red Flag Hold on the original student account in question, and begin a Red Flag investigation by the designated college official.
- If a staff member has been contacted regarding possible identity theft, the staff member needs to confirm the alleged victim's identity. If staff member cannot confirm identity through normal means and has reason to believe that identity is in question, the staff member needs to notify their direct supervisor immediately and a Red Flag investigation by the college will commence.
- If the Red Flag investigation results in fraud, a Red Flag Hold will be placed on the student's account, and the supervisor will report the situation to the college

disciplinary officer for follow-up as appropriate and to the College Program Coordinator for preventing identity theft.

- If situation is deemed to affect another student on campus, that student will be notified of concerns and given information about protecting their identity, including his/her right to a Privacy notice on their student account, creation of a new student account, etc.
- In all cases, the supervisor reviews the information/situation and notifies the College Program Coordinator within 3 working days.
- The College Program Coordinator will review the situation, contact all affected parties, give identity theft prevention information including option to notify local police, and add information to a standard tracking grid for reporting purposes. All reported situations will be tracked in this manner. The College Program Coordinator will inform CCCS Legal and CCCS Student Affairs apprised of any unusual patterns of activity regarding identity theft issues.
- If Financial Aid (FA) is involved, the Director of Financial Aid will utilize the FA and FD holds as appropriate, notify CCCS Legal and CCCS Financial Aid and make appropriate referral to the Inspector General's Office, U.S. Department of Education.

The Program Coordinator will submit the tracking report, and send comments regarding number of total incidents that were not resolved, the program effectiveness and program improvements to the CCCS Program Administrator by June 30th of each year.

APPENDIX III

Colorado Community College System

Identity Theft Prevention and Detection Program

All contracts with vendors have been updated with the following wording to improve compliance with GLB and state law.

NEW CONTRACT LANGUAGE:

A. "Incident" means any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access loss, disclosure, modification, disruption, or destruction of any communications or information resources of the State, which are included as part of the Work. Incidents include, without limitation, (i) successful attempts to gain unauthorized access to a State system or State information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; or (iv) changes to State system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent or disclosure of State Confidential Information or of the unauthorized modification, disruption, or destruction of any State Records.

B. "PII" means personally identifiable information including, without limitation, any information maintained by the State about an individual that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, all information defined as personally identifiable information in §24-72-501 C.R.S., student education records under FERPA, and nonpublic personal financial information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809, .

C. "Securely Destroy" means taking actions that render data written on media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the current National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.

D. "State Confidential Information" means any and all State Records not subject to disclosure under CORA. State Confidential Information shall include, but is not limited to, PII, and State personnel records not subject to disclosure under CORA.

10. CONFIDENTIAL INFORMATION-STATE RECORDS

A. Confidentiality

Contractor shall keep confidential, hold and maintain, and cause all Subcontractors to keep confidential, hold and maintain, any and all State Records that the State provides or makes available to Contractor for the sole and exclusive benefit of the State, unless those State Records are otherwise publically available at the time of disclosure. Contractor shall not, without prior written approval of the State, use publish, copy, or otherwise disclose to any third party, or permit the use by any third party for its benefit or to the detriment of the State, any State Records, except as otherwise stated in this Contract. Contractor shall provide for the security of all State Confidential Information in accordance with all policies promulgated by the Colorado Office of Information Security and all applicable laws, rules, policies, publications, and guidelines. Contractor shall immediately forward any request or demand for State Records to the State's principal representative pursuant to section 8B of this Contract. Contractor shall notify its employees that they are subject to the confidentiality requirements set forth in this Contract and shall provide each employee with a written explanation of the confidentiality requirements before the employee is permitted access to State Confidential Information.

B. Background Checks. Contractor represents and warrants that its employees have undergone appropriate background screening and possess all needed qualifications to comply with the terms of this Contract. For employees who create, obtain, transmit, use, maintain, process, or dispose of PII, State Confidential Information, or financial or business data which have been identified to Contactor as having the potential to affect the accuracy of the State's financial statements, Contractor will perform the following background checks on all employees who have potential to access such data in accordance with the Fair Credit Reporting Act and other applicable federal or state laws: Social Security Number trace; seven (7) year felony and misdemeanor criminal records, check of federal, state, or local records (as applicable) for job related crimes.

C. Other Entity Access and Nondisclosure Agreements

Contractor may provide State Records to its agents, employees, assigns and Subcontractors as necessary to perform the Work, but shall restrict access to State Confidential Information to those agents, employees, assigns and Subcontractors who require access to perform their obligations under this Contract. Contractor shall ensure all such agents, employees, assigns, and Subcontractors sign nondisclosure agreements at least as protective as those in this Contract, and that the nondisclosure agreements are in force at all times the agent, employee, assign or Subcontractor has access to any State Confidential Information. Contractor shall provide copies of those signed nondisclosure restrictions to the State upon request.

D. Use, Security, and Retention

Contractor shall use, hold and maintain State Confidential Information in compliance with any and all applicable laws and regulations in facilities located within the United States, and shall maintain a secure environment that ensures confidentiality of all State Confidential Information wherever located. Contractor shall provide the State with access, subject to Contractor's reasonable security requirements, for purposes of inspecting and monitoring access and use of State Confidential Information and evaluating security

control effectiveness. Contractor will store and process State Confidential Information in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alternation, and use. Such measures will be no less protective that those used to secure Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Contractor warrants that all electronic State Confidential Information will be encrypted in transmission (including via web interface) and stored no less than 128-bit level encryption. Contractor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Contract. Upon the expiration or termination of this Contract, Contractor shall return State Records provided to Contractor or Securely Destroy such State Records in the possession of Contractor and any subcontractors or agents to which the Contractor might have transferred State Records, and certify to the State that it has done so, as directed by the State. If Contractor is prevented by law or regulation from returning or destroying State Confidential Information, Contractor warrants it will guarantee the confidentiality of, and cease to use, such State Confidential Information.

E. Incident Notice and Remediation

If Contractor becomes aware of any Incident, it shall notify the State immediately and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, as determined by the State. Unless Contractor can establish that none of Contractor or any of its agents, employees, assigns or Subcontractors are the cause or source of the Incident, Contractor shall be responsible for the costs associated with the Incident, including but not limited to notifying each person who may have been impacted by the Incident, providing one year's credit monitoring to the affected individuals if the State Confidential Information exposed during the breach could be used to commit financial identity theft, and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as result of the Incident. After an Incident, Contractor shall take steps to reduce the risk of incurring a similar type of Incident in the future as directed by the State, which may include, but is not limited to, developing and implementing a remediation plan that is approved by the State at no additional cost to the State. Contractor will not provide notice of the Incident directly to individuals whose State Confidential Information was involved in an Incident, regulatory agencies, or other entities, without prior written permission from the State.

F. Disaster Recovery and Business Continuity Plan

Contractor represents and warrants that it has commercially reasonable procedures in place to prevent an interruption of service delivery under this Contract and a commercially reasonable disaster recovery and business continuity plan in effect in the event of a disaster. Contractor will notify the State of impending cessation of its business and any contingency plans. Contractor shall implement its exit plan and take all necessary actions for a smooth transition of service with minimal disruption to the State. Contractor will also provide a full inventory and configuration of servers, routers, other hardware, and

software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State.

G. FERPA Compliance

Contractor shall comply with the Family Education Rights and Privacy Act (FERPA) in its collection and use of Student Education Records. If Contractor will have access to Student Education records as defined under FERPA, the Contractor acknowledges that for the purpose of this Contract it will be designated as a "school official" with "legitimate educational interests" in the Student Education Records, as those terms have been defined under FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials. The Contractor will use the Student Education Records only for the purpose of fulfilling its duties under this Contract for the State's benefit, and will not share such data with or disclose it to any third party except as provided for in this Contract, required by law, or authorized in writing by the State. Contractor will return or destroy Student Educational Records within a reasonable time upon completion of this Contract, in accordance with the provisions of FERPA.

H. Gramm-Leach-Bliley Act Compliance

Contractor shall comply with the Gramm-Leach-Bliley Act (GBLA) in its collection and use of student financial data. The Contractor will use student financial data only for the purpose of fulfilling its duties under this Contract for the State's benefit, and will not share such data with or disclose it to any third party except as provided for in this Contract, required by law, or authorized in writing by the State. Contractor shall implement the Use, Security and Retention actions detailed in paragraph 10D with respect to the security of student financial data.

I. Protection of Personal Identifying Information

Contractor shall comply with C.R.S. § 6-1-713.5 in its collection and use of personal identifying information and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information received and reasonably designed to help protect the personal identifying information from unauthorized access, use, modification, disclosure, or destruction. In the event of a security breach that compromises the security, confidentiality, or integrity of personal identifying information, Contractor must immediately notify the State and abide by the notice provisions of C.R.S. § 6-1-716.