REQUEST FOR PROPOSAL #881609
ACCOUNT CLAIM AND IDENTITY VERIFICATION SOFTWARE
MANDATORY MINIMUM REQUIREMENTS

	Requirements	**Supplier Capability** (YES = **Y** or NO = **N**)	**Supplier Comments**
1.	Solution must support a production and one or more non-production environment(s).		
2.	Solution must support the following types of users: Admitted students, faculty, staff, alumni, retirees, and third party/non-employee.		
3.	Solution must allow different levels of identity assurance to be assigned based on account type.		
4.	Solution must support prevention of unauthorized access through robust identity verification mechanisms.		
5.	Solution must support a seamless, user-friendly interface for both claimants and administrators.		
6.	Solution must have a self-service portal for users to initiate account claims.		
7.	Solution must support integration with MSU's backend systems (Oracle DB, MSSQL DB, MySQL DB, API endpoints) for claim validation.		
8.	Solution must have a notification system (email) for claim status updates.		
9.	Solution must have the capability to expire account claim codes after an allotted timeframe.		
10.	Solution must support document upload and OCR capabilities.		
11.	Solution must have fraud detection and flagging for suspicious activity.		
12.	Solution must support multi-factor ID verification (e.g., government-issued ID, email/phone verification, address verification).		
13.	Solution must support government-issued IDs and address verification from		

	countries including and other than the United States of America.		
14.	Solution must support real-time and asynchronous verification workflows.		
15.	Solution must have the capability to display on-screen error messages when users enter information with formatting issues (e.g. incomplete email entries, incorrect DOB format).		
16.	Solution must adhere to accessibility guidelines and be WCAG 2 compliant.		
17.	Solution must adhere to relevant regulatory and privacy requirements (e.g. GDPR and FERPA).		
18.	Solution must provide multiple on-screen language options for end users.		
19.	Solution must have a responsive design compatible with desktop, tablet, and mobile devices, and varying browser types (e.g. Firefox, Safari, Chrome).		
20.	Solution must support use of international IP Addresses.		
21.	Solution must have an administrative dashboard for monitoring and managing account claims.		
22.	Solution must have access controls and role-based permission settings.		
23.	Solution must have reporting and analytics tools.		
24.	Solution must have a case management system including notes, history, and escalation paths.		
25.	Solution must allow case managers the ability to manually confirm identities as verified.		
26.	Solution must have cloud-based or hybrid deployment options.		

27.	Solution must have API access for integration with other systems.		
28.	Solution must have secure data storage and transmission (encryption in transit and at rest).		
29.	Solution must have audit trails for all user and administrative activity.		
30.	Solution must have an uptime SLA (e.g., 99.9%) and be scalable to handle peak demand.		
31.	Solution must be compatible with an external identity provider (e.g., SAML, OAuth, OIDC).		
32.	Solution must comply with industry standards (e.g., SOC 2, ISO 27001).		
33.	Solution must have clear escalation procedures with a dedicated account manager and customer support contact.		
34.	Solution must perform regular updates, patches, and bug fixes.		

Notes on terminology:

- OCR = Optical Character Recognition; “reading” text from images or scanned documents, and transforming it into machine-readable text
- WCAG 2 = Web Content Accessibility Guidelines (Version 2); Set of international standards created by the World Wide Web Consortium to ensure web content with accessible to people with disabilities
- GDPR = General Data Protection Regulation; A Comprehensive privacy law within the European Union
  FERPA = Family Educational Rights and Privacy Act; U.S. federal law for the protection of student educational records
- Uptime SLA = Service Level Agreement; commitment to ensure a specific level of system availability
- SAML = Security Assertion Markup Language; Single Sign-On utilizing XML to pass security information between an Identity Provider and a Service Provider
- OAuth = Open Authorization; Provides delegated access utilizing access tokens to protect a user’s password
- OIDC = OpenID Connect; Supports user authentication by providing an ID token to confirm users’ identity
- SOC 2 = System and Organization Controls (Version 2); U.S.-based auditing standards developed by the American Institute of CPAs
- ISO 27001 = International Organization for Standardization; International standard for protecting organizations’ sensitive user information