2020

Fraudulent Transcripts

Edward Trombley
Embry-Riddle Aeronautical University, tromblee@erau.edu

CHAPTER SEVEN

Fraudulent Transcripts

Edward F. Trombley III

REGISTRAR

~ EMBRY-RIDDLE AERONAUTICAL UNIVERSITY–WORLDWIDE ~

Fraudulent Transcripts

The use of fraudulent credentials, including standalone transcripts, forged degrees, and the transcripts that support forged degrees, is a concern worldwide, which affects colleges and universities, employers, governmental licensing boards, and other agencies. The circumstances are varied, the scenarios often implausible, and many fall into the "truth is stranger than fiction" category. Consider the following cases:

- At the newly created Department of Homeland Security, a candidate was hired to oversee its computer network as a senior director with a six-figure salary. The candidate had over twenty years' experience in federal IT system work, and was credentialed with bachelor's and master's degrees in computer science, as well as a Ph.D. in computer information systems. Unfortunately, a few weeks after hiring, the Office of Personnel Management opened an investigation into the new hire and found that all three degrees were from a degree mill operating out of a former Motel 6 in Evanston, WY (Risen 2006).
- A retired FBI agent, who spent 11 years with the department busting diploma mills, and who was at that time serving as his community's fire chief, admitted to a local news service that he had been lured into purchasing his degree online from a diploma mill based in Pakistan (Douglas 2017).
- A Florida State House candidate claiming to have earned a college degree, eventually revealed as a fake, attempted to weather the initial storm of publicity by submitting a photo posing with her diploma. Eventually, the candidate admitted the credential was forged and withdrew from the race (Phillips 2018).
- A North Carolina doctor was convicted of involuntary manslaughter and practicing without a license after taking a child off insulin, resulting in her death. The doctor possessed a fake medical degree (Risen 2006).
- Peter "Pete" Smith received his MBA from the American University of London, based upon his "previous experiential learning" and a payment of nearly $8000 USD. Though the University states that it requires applicants submit evidence of qualifications, as well as a photograph, Pete's failure to do so did not prohibit the awarding of his degree. Fortunately, Pete was never able to utilize the degree as intended, as the journalist reporting the story eventually disclosed that Pete is a pet dog (McLemee 2014).

Specifically, transcript fraud is the fabrication of a document purported to be a transcript from an accredited college or university, an alteration to an officially issued record, or the inclusion of courses and grades into the transcript that were not earned. Almost any document can be altered, even by a novice, due to the availability of professional grade desktop publishing and reproduction technologies for personal use.

Employers, colleges, and universities must exercise due diligence in verifying the credentials of potential employees or students. Technologies, including electronic transcript exchange, transcript security paper, and the National Student Clearinghouse's enrollment and degree verification services, have helped to reduce fraud and facilitate the credential verification process. Additionally, many schools have defined degree information as directory information, as permitted by FERPA, facilitating the confirmation of any credentials claimed.

Forging academic information may be considered a misdemeanor or felony depending upon the state in which it occurred, with penalties varying accordingly. Institutions that suspect or confirm academic fraud are encouraged to contact their local and/or state law enforcement should they wish to pursue investigation or prosecution.

Who Commits Transcript Fraud?

Transcript fraud exists at multiple levels, including incidents perpetrated by individuals, students, employees, management, licensed professionals, politicians, and even by companies whose business is the manufacturing of forged credentials. Institutional employees have access to data and the technology that can be manipulated for fraudulent use, as do student employees who assist with functions in a record's office. Setting up quality assurance processes and transactional reviews will help eliminate attempted fraud, as will yearly audits of staff who have access to update student records. A termination policy for staff members found to have altered official records should be put in place and strictly observed.

Student fraud has many facets and can range from academic dishonesty to altering one's academic history. Academic dishonesty can involve plagiarism of documents or papers and fabrication of information, data, or documents. Students' access to their own academic history through technology can also lead to the temptation to alter their academic record. Fraud also occurs when individuals take the identity and transcript of another student and present it as their own, affecting both the perpetrator and the victim whose record is stolen.

Institutional registrars, in their capacity as custodians of the academic record, bear the responsibility of ensuring the accuracy and authenticity of its history and content, specifically that the courses and grades earned in those classes are verified and legitimate. All colleges and universities should have policies and procedures in place to manage the various degrees of academic fraud, including how the outcome may, or may not, be annotated on the student academic record.

Some fraud occurs via companies that are willing to provide students with fraudulent documents for a price. In a CNN report, a board member of the Council for Higher Education Accreditation estimated that "more than 100,000 fake degrees are sold each year in the U.S. alone. Of those, around one third are postgraduate degrees. He added that bogus degrees will typically coast $1,000" (Tutton 2010). Hiring authorities are becoming increasingly aware of these diploma mills and their products, which may provide forged transcripts and/or credentials, and are verifying infor-

mation through the National Student Clearinghouse, licensing boards, and other record repositories.

The Office of the Registrar is essential in communicating the risks and penalties associated with fraud, and in monitoring for such fraud.

Ensuring Transcript Integrity

Registrars, in their role as data stewards for the transcript, must uphold the highest ethical standards to maintain the accuracy and integrity of the student record. Staff members in the Office of the Registrar must maintain the respect of their colleagues at the institution through careful data management practice and policy adherence, so that if/when an incidence of fraud occurs, they have established their credibility as data stewards.

It is imperative to identify the risks, as well as create, implement, and update a mitigation plan, which is reviewed and updated on a yearly basis, or as needed due to changes in policy, procedure, or technology. Some areas of risk include insufficient staffing, lack of secure storage, office space security, system security, reporting systems, and vendor security.

Paper Transcripts Produced In-House

Colleges and universities often produce their own paper transcripts in-house, both for speed and ease of order fulfillment. Additionally, institutions retain the ability to quality check transcripts for content and completeness before issuing. Institutions who choose to issue their own paper transcripts must take precautions to ensure the potential of fraud is minimized in the transcript production process. A procedure should be documented and reviewed regularly, particularly if a third-party service provider is utilized to facilitate the ordering of transcripts and collection of fees, as most companies routinely implement updates. The procedure should include a provision to maintain a copy of the signed transcript release, including the designated recipient, in the student file for as long as institutional record-keeping policies require.

Print official transcripts on security paper. The secure paper should include multiple security features. Many options are available when selecting and configuring features for institutional paper, but best practices include:

- Institutional identification should appear on the official transcript via printing at the campus, or preferably before printing, at the manufacturer;
- Registrar's signature and the institutional seal embossed, imprinted, generated, or preprinted on the transcript stock. In the 2019 survey to collect transcript practices, 98 percent of institutions responded that the registrar was the "position and person's signature" on the transcript, establishing this as standard practice (AACRAO 2019a);
- A detailed transcript key should be pre-printed (usually on the back of the paper) and should include descriptions of the verification features. Seventy-two percent of survey respondents reported that their institutional transcript's key included the method of certification in the key of the official transcript (AACRAO 2019a);
- Transcript paper that is difficult to replicate. Employ multiple security features, including options such as thermochromic ink, watermarks, foil holograms, latent images that appear when documents are photocopied or scanned, micro-printing, fluorescent fibers, etc.;
- Transcript paper that is difficult to alter or strip of content. To prevent the bleaching or lifting of imprinted information on a transcript, paper may be made chemically sensitive to bleach or solvent, and contain toner adhesion properties that prevents the scraping or lifting of toner with tape.

Transcript production access, including access to the transcript paper, letterhead, pre-printed envelope stock/mailers, and the institutional seal, should be limited. All staff and student employees involved with transcript production should undergo criminal background checks prior to employment and should be provided FERPA training before being given security rights to access institutional records. It is recommended that all staff and student employees sign confidentiality, and appropriate use, agreements each year. For a sample of an employee confidentiality agreement, *see* Appendix H, on page 165. Make every effort to ensure adequate office security (*see* "Employees and Desk Space Security" on page 64).

An employee, rather than a student staffer who might be transitory or subject to influence by fellow students, should review transcript requests for processing, regardless of whether a request is a drop-off in the office, via the mail, or electronic. A limited number of trained staff members should have this responsibility. When producing paper transcripts it is important to:

- Review requestor and recipient information for accuracy and FERPA compliance. (*see* "The Family Educational Right and Privacy Act" on page 54).
- Process the transcript request, ensuring an audit trail is available.
- Issue official transcripts in official envelopes, bearing the designation "Official Transcript." A date of issue should also be included on the transcript. Mark "Issued to Student" on each page of any transcript that has been given directly to, or mailed directly to, the student. Warn the requestor that, as a security measure, some institutions now refuse any transcript bearing this designation.
- Maintain a copy of the signed release, including the designated recipient, in the student file until the administrative need for the release is satisfied.

Paper Transcripts Produced by a Third Party

Many colleges and universities contract with third party vendors not just to manage requests for, but also to produce and distribute official transcripts. Record stewards are encouraged to consider if their institutional records require routine manual intervention to correct transcripts prior to production, due either to data entry error or prior student system conversion errors. If this is the case, the process of printing and distributing transcripts might be best kept in-house. Before signing a contract with a vendor, it is important to have the institution's general counsel review the terms, to ensure the institution's data integrity protocols are followed. It is important to establish a documented process with the vendor, in either the contract or statement of work, which prevents fraud.

Contractual components to look for include:

- Security of data as it is transferred from the institutional data source to the vendor, and from the vendor to the transcript destination
- Security breach protocol, including notification of any breach, so that the institution may assess FERPA liabilities.
- Opportunity for quality assurance review of the vendor by the institution.
- A specified processing time, with consequences if timelines are not met, such as compensation to the institution and/or to students impacted.
- Review of negotiated contract timing, as well as renewal options.
- Pricing variance regarding varied production numbers, handling of remitted fees, and revenue collection mechanisms utilized by the vendor.

- Right to terminate contract for unsatisfactory performance.
- Easily accessible reporting of performance to the institution.
- Vendor requirement to retain or remit a copy of each signed release collected, including the designated recipient, for the student permanent file to be kept until its administrative need is satisfied.

Electronic Transcripts Produced In-House

Electronic transcripts provide several added security benefits over paper transcripts. The potential for error in data entry is largely eliminated, the sending institution can be verified, the date of receipt can be confirmed, and the transcript can be certified as authentic and without alteration. *See* Chapter 5, "Electronic Transcripts" for more information about record security. For electronic transcripts produced in-house, the following precautions should be employed:

- Create an authenticity verification process for both incoming and outgoing transcripts.
- Assure the secure transfer of electronic information, utilizing a file format that is not alterable, in coordination with security protocols dictated by institutional information technology resources.
- Create audit trails for quality assurance review in tandem with institutional information technology resources.
- Maintain a copy of the signed release, including the designated recipient, in the student file for retention until the administrative need for the release is satisfied.

Electronic Transcripts Produced by a Third Party

Third-party vendors should be held to the highest standards, with the following security measures in place:

- Ensure that the vendor takes precautions to protect against fraud by their own employees, and that their staff are FERPA trained and compliant.
- Request a copy of the vendor's employee ethics statement as well as policies and procedures regarding data integrity.
- Review vendor quality assurance and security processes for sending electronic transcripts to recipients including students, employers, and other educational institutions.
- Review vendor processes, quality assurance, and security measures for electronic transcript retrieval by recipients.
- Ensure that the transcript will reach the ultimate destination in an encrypted format, and once accessed, the vendor system should produce a residual record of who downloaded the document, as well as the date and time.
- Request fraud protection documentation.
- Request authenticity verification, security protocol, and quality assurance documentation for review.
- Require the vendor to retain or remit a copy of each signed release, including the designated recipient, to be kept in the student file until the administrative need for the release is satisfied.

Unofficial Transcripts Produced by Students

Technological advances in student information systems now generally permit students access to their academic history, and offer the ability to produce and subsequently send unofficial transcripts to potential employers, third party sponsors, or other schools often at no cost. The sophistication of current desktop publishing technologies, coupled with the fact that unofficial transcripts are generally produced on plain paper, means that students can manipulate, alter, or forge their academic history more easily than in the

past. Companies and institutions should be aware of this potential and have processes in place to prevent or identify such fraud, and to respond to fraud when it is reported. At a minimum, student generated unofficial transcripts should be designated as such, and should include identifying information on each page so that a recipient can reach out for verification if unsure of documents authenticity. Institutional policies regarding the ramifications of students altering their academic records, up to and including dismissal from the institution, should be clearly communicated.

Identifying Fraudulent Transcripts

Transcripts received from other colleges or universities should be reviewed for authenticity before evaluation and inclusion in the permanent student record. Additional screening should occur if the transcript comes directly from a student. Indeed, some institutions will no longer accept as official a transcript that has been in the hands of a student, even if it is presented in a sealed envelope. When fraud is suspected, the Office of the Registrar staff should work directly with the presumed sender to determine the validity of the transcript.

Reviewing for the following "red flag" elements can assist in determining if a transcript has been altered:

- Illogical data elements,
- Unacknowledged attendance gaps,
- Suspect grade changes,
- Blank or missing grades,
- Degree awarded does not appear to match coursework completed,
- Unclear or suspect signature,
- Inaccurate transcript key,
- Changes in font or font size within the body of the transcript, particularly among the data elements including course number, course title, grades earned, quality points, GPA, and degree conferral information,
- Irregularities in layout, including variances in spacing, page breaks, margins, etc.

Additional items to verify authenticity if a paper copy is provided:

- Transcript is in official institution envelope with seal present and intact,
- Transcript arrived from an accredited institution or established third-party vendor,
- Postmark is appropriate to the institution or vendor,
- Security paper is used, with features corresponding to those noted in the security paper description in the key,
- Transcript key or legend is present, complete, and corresponds to the transcript content,
- Institutional certification is present on the document, with contact information for the institution included,
- Transcript has a recent date of issuance.

International Transcript Fraud

Transcripts from international entities are more challenging to check for authenticity and alteration. In some parts of the world academic records fraud is more common, such as western and central Africa and the Caribbean. Fake international transcripts are generally nearly identical to original transcripts, and can include emblems, seals, and high-quality paper. Institutions should require that all incoming official transcripts be sent directly from the issuing college or university or, at a minimum marked "issued to student," in a sealed envelope. If an international evalu-

ation service is used to authenticate, translate and/or evaluate an international credential, to assure the highest level of confidence in the resulting report, it is preferable that the vendor who provides the service maintain membership in the National Association of Credential Evaluation Services (NACES).[12] AACRAO provides significant resources to assist in identifying fraudulent transcripts. AACRAO also provides information about web-marketing techniques used in diploma sales, state and federal laws, resume fraud, and employer verification.[13]

Diploma Mills

There are many entities around the world that produce and sell documents that appear to be academic credentials, such as diplomas, degrees, and transcripts, from what appear to be colleges or universities, but are in reality academically worthless documents from fictitious, or "shell" educational institutions, also known as diploma mills. Diploma mills are a profitable industry, with an estimated annual revenue of $200 million. Estimates suggest that 500 Ph.D. degrees are awarded monthly, from approximately 400 diploma mills, functioning under the "authority" of an estimated 98 fake accrediting agencies operating within the United States today (College Choice n.d.).

Protecting institutions and workplaces from falling victim to this kind of academic fraud can be promoted by educating staff about the warning signs commonly associated with fake credentials. Some of the most common signs of diploma mill fraud include:

- Time to degree completion: It is unlikely that any legitimate degree can be earned in days, weeks, or a few months.
- Institutional domain names that do not end in .edu: While some schools still in the accreditation application process may not have a .edu domain, non-'.edu' entities warrant further investigation. "Before the U.S. Department of Commerce created its current, strict requirements, some questionable institutions were approved to use an .edu. The current requirements allow only colleges and institutions accredited by an agency recognized by the U.S. Department of Education to use the .edu, however, some more suspect institutions have maintained the .edu addresses." (U.S. Department of Education 2009).
- Complaints with the Better Business Bureau (BBB): Although many accredited schools may have complaints against them, reviewing reporting from the BBB to establish institutional legitimacy is suggested.
- Tuition paid on a per-degree basis: Most legitimate institutions charge by the credit hour, course, semester/quarter, or the year.
- Lack of a physical address: Legitimate schools or colleges publish their address, phone number and other information on their transcripts or in transcript keys. A school that only provides a website for contact information may indicate a fraudulent entity. Similarly, a school whose address is a PO box number or single suite may well be a masking entity with no physical presence.
- Similar name to a well known school, such as Columbia State University (mimicking Columbia Southern University or Columbia State Community College), University of Britain (mimicking the University of London, Manchester, Cambridge, etc.) or Oxford England University (mimicking the University of Oxford).
- Lack of state licensing or nationally or regionally recognized accreditation: Rather than accred-

[12] This may be ascertained by reviewing the membership directory on the NACES website <naces.org>.
[13] *See*, AACRAO's website <aacrao.org> for a complete exploration of these topics.

ited, diploma mills often claim to be "authenticated, verifiable, licensed, notarized [or] internationally approved" (College Choice n.d.). Such information can be verified via the U.S. Department of Education.

- Hundreds of degree programs: Many larger reputable schools only offer one hundred degrees or fewer.

Using a methodical approach to review incoming transcripts is essential to identifying whether the documents presented are from a real, legitimate, and appropriately-recognized institution.