

Education Sector Case Study

Large Institution Addresses Document Security Issues

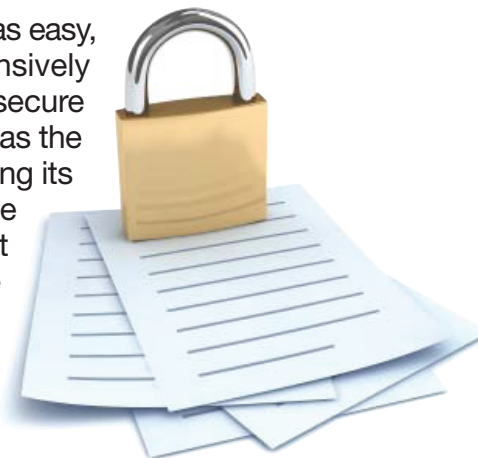
The customer is a large post-secondary institution offering a wide range of courses, primarily in business and technology, though other disciplines are present. This institution has a significant number of students from outside the province including a number from international destinations.

The Need – over the years, several incidents and practices have impacted the reputation of the institution within the industry and more significantly with employers and with government agencies. Anecdotal evidence indicates that graduating students have been modifying the transcripts that they have been supplying to employers as part of the hiring process. Usually the transcript has been modified to adjust the marks but in the past year it seems that some students are using a cut and paste technique to even change the courses they took thereby making them appear even more attractive to the employer in the current tough job market. Consideration has been given to providing the employers with transcripts directly however issues of confidentiality and release of information have made the process too difficult to implement and manage. Furthermore, the majority of employers are requesting this information from the job applicant and are expecting it to come from the student and not the university directly. Currently, students order one copy of the transcript and make as many copies as they want to provide to employers when requested.

In the past several years a larger problem has begun to surface regarding admission letters. Overseas students, like the ones within the province, receive a letter of admission inviting them to study at the institution in the coming fall. This letter is being photocopied and taken to the local embassy where it is being used as supporting documentation for gaining a student visa for not only the accepted student but others with the same or similar name.

A threat risk analysis was conducted which concluded that although the risk of document copying and fraud was only moderate and not directly impacting the financials of the institution, the reputation of the institution was suffering. Taking no action to address this issue was not considered to be in the best interests of the school. The Board of Governors had also become interested in the matter as this was seen as another instance of identity theft and was querying their personal liability and culpability as Directors if no action was taken.

Options Considered – Admission Letters and Transcripts were seen as easy, quick wins if authenticable documents could be simply and inexpensively produced. Initial consideration was given to printing on pre-printed, secure paper, however, this increased the cost and the security requirements as the institution determined that it needed its own special security paper using its own logo rather than using commercial variants. This would have required the printing of a large stock of paper, entailing a significant up front cost, plus there was an issue of how best to store and secure the pre-printed stock. Use of specialized paper with taggants or imbedded threads was even more expensive and had the same



issues with respect to storage and security. In all cases, the use of special paper required that a machine be pre-loaded with it or paused until the proper paper could be inserted which was viewed as a detriment to the smooth administrative flows within the office. The printers used for these letters and transcripts were not dedicated to just these tasks.

The Solution — after due consideration of the alternatives, the school chose to implement Digital Void Pantograph (DVP) and Digital Verification Grid (DVG) technologies on a number of their digital presses.

When copied, the DVP displays a “VOID” or “UNAUTHORIZED COPY” logo across the page. The DVG that was present on the original and included the school’s logo disappears on the copied version. Because the DVG also is a continuous pattern, the cut and paste technique of creating a bigus transcript was foiled.

This resulted in a significant cost savings compared to other options as only plain paper is used in the production of the documents. No additional up front costs, nor special inventory controls or storage costs were required. Working with the vendor, the DVP/DVG incorporated the school’s logo as part of the design thereby providing additional security and uniqueness to their documents. Additionally, by adding a color stripe to the document, further security against tampering and copying was achieved as only color copiers could reproduce the document, but in attempting to do so, they triggered the anti-copy features of the DVP and DVG.

As a result of the implementation the two key issues concerning Transcripts and Admission letters have been satisfactorily addressed with minimal cost. Students are no longer able to produce transcript forgeries that could pass as originals. The ability to cut and paste from several documents to produce a forged version is no longer feasible. The ability to copy Admission Letters to use as documentation for obtaining a student visa is no longer possible.

Two unanticipated side benefits occurred as a result of the implementation. The school was able to actually reduce the cost of the Transcript because students were no longer able to make suitable copies for themselves. Even at the reduced cost, the total revenue received by the school has increased. Because the transcripts are being printed on plain paper, there is a pilot project to permit students to request copies at a self-serve kiosk to provide improved customer service and turnaround times.

Within the office environment, the implementation of the DVP and DVG for the Admission Letters has facilitated the use of these technologies on other documents such as tests, lecture material and parking passes for the residences where copies had become a significant issue. The Arts Society is incorporating the technology into its tickets for a coming series of concerts where, in the past, there have been some issues with forged tickets.

Bottomline — the problem was solved in an inexpensive way without any significant technology implications. Workflows did not require significant change and the users of the output have expressed no complaints or misgivings (except those that used to commit the forgeries).