Avoiding an Identity Crisis: Why Advanced Visual Security is a Critical First Line of Defense

Author: Josh Nippoldt, Senior Product Marketing Manager
Publishing: June 15, 2015

Advanced Visual Security Features Help to Protect Your People and Your Property

With headlines in the news about terrorist attacks, shootings at schools and hospitals, and rampant identity fraud, security has become top of mind no matter where you go or what you do today. In virtually every aspect of life, some sort of identification is required – whether it’s a passport, driver’s license, employee credential, student ID card, or proof of insurance.

To prevent fraud, ID cards are getting more sophisticated, with specific text or embedded data that helps confirm the identity of the cardholder. However, these unique identifiers are only useful when the person checking ID cards has the right tools, such as specialized hardware readers or access to databases, and the training to use them. Without the proper tools and training, it is exponentially more difficult to validate that the card has not been forged or stolen, and that the person possessing it actually is who he or she claims to be.

That’s when visual security becomes a critical first line of defense. Individuals in high-security facilities need to be able to easily and readily identify that the person holding an ID card is, in fact, the legitimate cardholder. Not only do these visual security elements protect the cardholder’s identity, they also reduce an organization’s risk associated with counterfeiting – whether it is prohibiting access to the wrong person, preventing health insurance fraud, or stopping the purchases of weapons by unauthorized individuals.

The Importance of Visual Security

Today’s ID cards are increasingly sophisticated with a number of high-tech features that have been designed to prevent counterfeiting and provide several different types of data to identify the individual cardholder. Many of these features, however, require expensive and proprietary validation equipment, and in some cases additional hardware, such as biometric readers, to verify the authenticity of the ID card. In other cases, third-party databases need to be consulted to confirm that the card hasn’t become compromised when it was lost or stolen. Therein lies the fundamental problem.

Consider a security guard working at a remote border crossing, the receptionist at a doctor’s office, or a student working as a desk clerk at a college dorm entrance. These individuals may not have the tools to read data embedded in an ID card, and if they do, they may not know how to properly use these often-sophisticated readers.

Because of these challenges, most people use a simple image to confirm the identity of a
cardholder. In fact, around the world, it is estimated that more than 90 percent of identity inspections are undertaken visually and in the field. Visual security has become a critical tool for those on the front lines because it:

- Is fast
- Cost-effective
- Convenient
- Minimizes training
- Eliminates the need for specialized hardware

A Growing Demand for Advanced Visual Security

While an array of users rely on visual security features today, these elements on ID cards are becoming increasingly important for governments, healthcare providers and insurers, and educational institutions. In this section, we’ll examine why these three market segments, in particular, are looking at advanced visual security options to deliver greater protection to people and property.

Government Agencies

The primary security concern of government agencies is protecting their citizens, legal foreign residents and employees, as well as highly secure government facilities. In addition, they seek to reduce the incidence of government-funded benefits fraud, enforce laws and secure borders, while containing, or even reducing, their technology costs. These activities have become more important in the last decade, as budgets have been slashed dramatically, identity fraud has been on the rise and targeted terrorist attacks have become more frequent and increasingly violent. Government agencies must therefore take every effort to ensure that they know who is entering or exiting a country or a building, purchasing weapons, and/or utilizing their services.

Take, for example, that there are an estimated 11.4 million unauthorized immigrants living in the United States\(^1\), which is creating a unique challenge for those guards stationed in border outposts, where their ID-reading hardware may not always be operational or even available to confirm the validity of each person’s ID. In those situations, the most accurate way to confirm that the person seeking to enter the country is who he or she claims to be is by a picture ID. But the use of counterfeit IDs to enter the United States continues to run rampant. In the summer of 2011, the U.S. Custom and Border Protection lamented about the surge of counterfeit IDs coming from overseas. In just the first half of that year, they caught about 15,000 counterfeit IDs, when in past years, during the same period of time, they’d typically only see 10 to 15.\(^2\)

---


\(^2\) Chicago CBP Officers Seize Unprecedented Number of Counterfeit Drivers Licenses. U.S. Customs and Border Protection, August 2011
But protecting the borders is not the government’s only need for advanced visual identification features as a line of first defense. These tools are vital for allowing entry to government buildings – whether the person is an employee, a contractor or a visitor – and providing social services, such as healthcare and welfare benefits.

Advanced visual security features on government-issued identification documents – including driver’s licenses, residency cards, weapons permits, employee or contractor IDs, or multipurpose cards for social services – can provide agencies with the confidence that they have tamper-proof digital technology that cannot be fraudulently altered, accidentally deleted, or otherwise accessed by unauthorized entities.

Healthcare

Whether healthcare services are privately managed, like in the United States, or run by the government, as it is in Canada and many European countries, similar challenges exist with regard to preventing medical identity theft and ensuring the privacy of those insured.

Healthcare fraud is a significant problem and one that involves a larger cost than was previously thought. According to a recent report by BDO, a leading accountancy and business advisory firm, and the University of Portsmouth’s Centre for Counter Fraud Studies (CCFS), in the past, “…organizations have either denied that they had any fraud or planned only to react after fraud has taken place. Because of this, fraud is now one of the great unreduced healthcare costs.” In fact, looking at more than 15 years worth of data, and a current global average loss rate of 6.99 percent, the report estimates that losses due to fraud total about $487 billion.³

In attempts to avoid medical identity theft and limit liability, hospitals, clinics, doctors’ offices and pharmacies now require picture ID when an insurance or healthcare benefits ID card is presented. But both the insurance cards and photo identifications could be susceptible to counterfeiting, still leaving healthcare organizations unprotected from the significant costs attributed to fraud they were hoping to deter.

There currently is an ongoing movement to create a Voluntary Universal Healthcare Identification (VUHID), which is based on two ASTM International E 31 standards to make globally unique healthcare identifiers available to any person who wishes to have one.⁴ The VUHID is a simple, inexpensive and reliable solution for both improving the accuracy of patient identification and providing additional privacy protection for healthcare information. It is designed to provide unambiguous patient identification; error-free linkage of clinical information; and enhanced privacy of patient information. It also will help reduce the rate of medical errors, decrease the incidence of healthcare-related identity theft, and help control healthcare costs. One critical element to making these cards work effectively is the inclusion of a tamperproof and non-creatable visual image of the patient that will help ensure that the cardholder is the individual intended to receive the healthcare benefits.

³ The Financial Cost of Healthcare Fraud 2014: What Data from Around the World Shows. BDO and The University of Portsmouth’s Centre for Counter Fraud Studies (CCFS), March 2014

⁴ The Voluntary Universal Health Identification (VUHID) Project: Improving Patient Safety While Protecting Patient Privacy. The Robert Wood Johnson Foundation, August 2014
By adding advanced visual security features to these health insurance cards, medical providers and government-run healthcare organizations can reduce identity fraud and simplify the lives of the patients they serve. Additionally, including a high-definition image of the policyholders on their insurance card ensures that the insured individual can be positively identified at his or her healthcare provider’s office, the pharmacy or the emergency room.

Education

Campus security is top of mind, particularly with a rise in on-campus violent crime and theft. But physical security to prevent the access of individuals perpetrating these crimes is not the only concern when it comes to IDs for students and university employees.

As the university market becomes more technologically savvy, forward-thinking institutions are enabling students to use their traditional ID cards for a wider variety of purposes – from dorm access and meal purchases, to transportation and financial transactions both on and off campus. With these converged cards, the implications of student ID fraud have grown. It’s no longer a matter of using student IDs to simply ensure that an individual has a legitimate purpose for being on campus. Fraudulent use of IDs can result in universities – and parents, students, teachers and administrative staff – losing significant amounts of money in their cafeteria or school store programs, or from personal banking accounts becoming compromised.

In addition, both parents and students place a high level of value on safety. Universities that employ leading security technology have a competitive edge over those that do not. By leveraging advanced visual security features on students’ “smart” ID cards, universities can enhance their brand image with greater personalization and stronger security for those in their campus community. Advanced visual security tools are a natural complement to many of the newer data storage technologies that universities are now using to replace conventional, and less secure, magnetic stripes on their student and staff ID cards.

Challenges of Implementing Visual Security Features

While the need for advanced visual security on identification documents is clear for government, healthcare, education and other markets, there are some challenges that arise as organizations seek to implement these features.

When IDs contain the same visual security element, such as a hologram, in the same location on each card, they can become an easy target for counterfeiters. Some types of holograms can be replicated so that upon visual examination, they look like the real thing. Once this copy is created, it can be difficult to stop counterfeiters from easily making thousands of duplicates of the ID.

Having a unique visual security solution – such as a recorded image of the cardholder – on each ID is preferred because it makes counterfeiting more difficult and helps those who are checking identification ensure the card’s validity. Laser engraving and optical security media (OSM) are proven means of providing a high level of visual security on an ID, but each of these solutions can

5 How Secure IDs Can Protect Campuses and Provide Other Benefits. Campus Safety Magazine, August 2014

6 Stemming the Tide of ID Theft at Institutions of Higher Education. Campus Safety Magazine, July 2011
have a high total cost of ownership. As a result, these solutions, while highly secure, have largely been restricted to only the most high-profile government ID programs, such as the U.S. Permanent Resident Card or “Green Card,” though a variety of organizations could benefit from the additional security that such personalization enables.

**Advanced Personalization from a Cost-Effective Platform**

HID Global® is addressing the need for more cost-effective, yet highly secure, personalized visual security elements with the introduction of vanGO®, a new portfolio of One-2-One™ visual security features that provide a level of ID personalization that is not possible with conventional holograms and at a cost of ownership that is significantly lower than laser engraving. The vanGO solution enables users to, on the spot, create cards that are highly counterfeit resistant and personalized to reflect the individual identity of the cardholder.

vanGO is setting a new standard in the development of personalized IDs. With new technology that enables users to write and physically embed a cardholder’s facial image on the card, vanGO makes it very easy for users to visually identify and authenticate the cardholder’s identity without electronic readers or access to databases. The One-2-One relationship between the card and the cardholder created by vanGO is nearly impossible to counterfeit. In fact, vanGO utilizes many of the same cutting-edge technologies found in HID Global’s LaserCard® Optical Security Media (OSM), for which there is no known instance of compromise.

HID Global uses an optical laser writer and unique materials to create images with up to 10,000 DPI on the vanGO media, which is a metallic patch that is hot-stamped onto an ID card.

**Conclusion**

vanGO is an ideal solution for the government, healthcare and education markets because it enables creation of tamper-resistant security that can be instantly personalized, issued quickly, and still allows for easy visual authentication by inspectors. In addition, the lower cost of vanGO, compared to traditional laser engraving and OSM alternatives, will make it possible for more widespread use throughout these organizations, even at a time when budgets are tight.

If you’re interested in learning more, please visit HID Global’s website for more information. Or contact us to find out how HID Global can help you create a custom solution designed specifically for your security needs.