Exponent®

THOUGHT LEADERSHIP

PUBLISHED 2Q 2019

Considerations for Counterfeit Prevention and Document Security

June 18, 2019

Technological advances have contributed to an increase in the manufacture and sale of counterfeit goods estimated to account for 2.5% of world trade in 2016, or $461 billion.[1] Over the past decade, developments in computer and printing technologies have made the forgery of secure identity documents such as passports, driver's licenses, and credit cards significantly easier, increasing the risk of identity theft. The International Criminal Police Organization (Interpol) claims that if left unchecked, the circulation of counterfeit currency and fraudulent use of identity documents could "undermine national economies" and pose "a major threat to society as a whole," respectively.[2]

While creating a document that is completely resistant to counterfeiting may be next to impossible, important materials and security features considerations can increase the time, cost, and effort required for a potential counterfeiter to illegally create or replicate a secure document. Examples include leveraging polymer-based substrates; having an intimate understanding of the materials chemistry; and incorporating the right combination of security features to securely meet an end user's needs. Document designers who identify advantageous combinations of these three elements can help increase the barriers to entry for counterfeiting.

Use of Polymer-Based Substrates

The transition from paper-based documents to polymer-based substrates is one important way the secure identity document industry can stay ahead of counterfeiting. Polymer-based substrates such as polycarbonate and polyvinyl chloride (PVC) can increase a document's durability and physical longevity, while also enabling the incorporation of security features that are incompatible with paper. For example, security features can be embedded into the multiple layers of printed text and background artwork that are stacked and adhered together in a polymer credential, such as a U.S. driver's license. It is possible to embed security features into paper, as is currently done with the security strip on the U.S. one-hundred-dollar bill. However, polymer-based substrates offer the opportunity to embed these features more easily. For this reason, many countries have transitioned or are transitioning both their currency and other secure documents, such as passport data pages, to polymer-based substrates that can be more challenging for counterfeiters to both source and produce.

Understanding of Materials Chemistry

Understanding the materials chemistry of the component parts of the secure identity document is another important consideration for optimizing document security and quality. If a document manufacturer is creating a multi-layered product, for example, it is important that the individual layers be free of contamination and chemically compatible with one another to allow for lamination. Inks and other security features must be appropriately selected for the application to avoid impeding the lamination process. If a document manufacturer

[1] "Measuring the Magnitude of Global Counterfeiting: Creation of a Contemporary Global Measure of Physical Counterfeiting," Global Intellectual Property Center, U.S. Chamber of Commerce, 2016.

[2] https://www.interpol.int/Crimes/Counterfeit-currency-and-security-documents

overlooks these considerations, the layers of the end product may be easily pulled apart, reducing the document's longevity and increasing its vulnerability to counterfeiting.

Similarly, it is important for secure identity document manufacturers to understand how the ultraviolet curing process used for the inks on the printed substrates can affect the surface chemistry of that substrate and how that may impact material compatibility in the end product. The lamination process may additionally affect the integrity of embedded security features if the materials are not optimized for the process being used. Additionally, the desired appearance of laser engraving on the finished document may not be achieved if the substrate chemistry is not formulated correctly. If a secure document manufacturer overlooks these considerations at the onset of the process, additives may need to be reconfigured or other downstream changes made to achieve the desired end result. Understanding the materials chemistry at the beginning of the document design process is critical to ensuring that elements are optimized to work together correctly.

Security Features Mix

Optimizing the type of security features and their interaction with one another can also help deter counterfeiters. Features can be classified into one of three levels depending on the level of security they afford. Level one features are visible by the human eye and include printing, some micro-text, and optically variable devices such as the security strip on the U.S. one-hundred-dollar bill. They can also incorporate a tactile element, such as intaglio printing or the laser engraving of personal information that can be both seen and felt on many U.S. driver's licenses and credit cards. Level two features require some type of simple equipment to view. Examples include inks that are visible under an ultraviolet light and microtext that requires a magnification device such as a magnifying loupe to view. Level three features have forensic attributes that typically require more sophisticated equipment that is inaccessible to the average individual. This includes features like taggants, anti-Stokes inks, or nanotext/nanoimages that can only be seen via spectroscopic characterization or high-magnification imaging. The difficulty of detecting these elements increases the likelihood that a counterfeiter may be unaware that they have been incorporated into the document.

It is important to note that, in general, a single security feature will not prevent a document from being counterfeited. Rather, it is how the security features interact with one another, the substrate material, and the artwork that enhance the complexity of the document. At the same time, it is important for document designers and manufacturers to ensure that the selected substrate, artwork, and security elements align with the primary needs of the end user. A credit card holder, for example, needs the security chip to be readable each time it is inserted at a retail store. A driver's license holder needs their personal information and photograph to be easily viewable so that their identification can be quickly verified. As document designers are selecting the raw materials and features for a secure identity document, considerations should be made to ensure it is both secure and suitable for its intended use.

Exponent's Expertise

Exponent's multi-disciplinary team of scientists, engineers, and cybersecurity experts evaluate materials chemistry, conduct durability testing, and partner with producers of credit cards, driver's licenses, passports, and other secure identity documents to optimize their security in both physical and electronic formats around the globe.

Sarah M. Conron, Ph.D.
Statistical & Data Sciences
Managing Scientist
Bowie
(301) 291-2556 | sconron@exponent.com

Exponent Office Locations
Atlanta, Austin, Boston Area (Maynard, Natick), Chicago Area (Downtown Chicago, Warrenville), Denver, Detroit, Houston, Miami, New York, Philadelphia, Phoenix, Northern California Area (Menlo Park, Oakland, Sacramento), Seattle, Southern California Area (Los Angeles, Orange County, Pasadena), Washington DC Area (District of Columbia, Maryland, Virginia)

International Offices:
Basel, Switzerland; Derby, Harrogate and London, UK; Düsseldorf, Germany; Shanghai and Hong Kong, China

www.exponent.com

Exponent®