W16 Technology and Design of Security Documents for Counterfeiting and Alteration Resistance

Joel A. Zlotnick, MSFS, United States Department of State, Washington, DC 20522; Dennis J. Ryan, MBA, Applied Forensics LLC, East Meadow, NY 11554*

Learning Overview: After attending this workshop, attendees will understand two facets of document security. First, this workshop provides an overview of common document security features, such as security fibers, watermarks, microprinting, color shifting inks, ultraviolet printing, holograms, laser engraving, and many others. The second and equally important subject is how document components can be integrated with one another, and with document artwork, in ways that allow the security value of each anti-counterfeiting technology to be maximized.

Impact on the Forensic Science Community: This workshop will impact the forensic science community by providing document examiners and other forensic scientists with a better understanding of how security documents are designed and counterfeited, improving the ability of examiners to differentiate between genuine and counterfeit.

Document counterfeiting remains a persistent problem for governments and the private sector alike and has produced an explosion of development in anti-counterfeiting technologies in recent decades. These include innovations in paper and plastic substrates, security inks, specialized printing technologies, holograms and other classes of features used in security documents, such as banknotes, passports, identity cards, and birth records. However, security feature technologies are often regarded as simple checkboxes, where a specific security feature technology is either included or not included in a security document design. In this context, the focus is often limited to ensuring that the document contains some designated minimum quantity of security features. Some attention may also be devoted to how various features fight against counterfeiting and/or alteration, but usually only within the limited scope of the feature's primary function. Certainly, technology selection is an important first step and does have broad consequences with regard to a security document's cost and manufacturability. However, security features are not integrated in the same way in every unique document or by each document issuer, so not all implementations of security feature technologies are equally effective.

Specifically, security feature technology selection alone does not account for how security design strategies can make or break the value of a technology and, by extension, the security of the document. Thoughtful and purposeful use of security feature technologies can maximize their effectiveness by integrating them with other document components, facilitating easier inspection by document users, or allowing each feature to generate additional value by occupying ancillary security roles that extend its functionality. For example, watermarks are a foundational security feature that have been used to protect paper substrates from counterfeiting for hundreds of years. Yet many modern watermark implementations allow a watermark to fill not only its primary role of deterring substrate counterfeiting, but also new roles as an anti-alteration feature. Other watermarks occupy unprinted areas of paper to signal document users that a watermark is present, and further use the watermark design to communicate specific information about the document issuer or purpose, both of which contribute to the ergonomic accessibility of the feature. Similar thinking can be extended to many other security feature technologies, such that the utility of each can be maximized with the help of specific design strategies relevant to each particular technology. In contrast, poor security feature implementations can waste resources, create a false sense of security, confuse document users, or even expose the document to counterfeiting or alteration risks.

This workshop will provide attendees with a two-sided view of security document design. First, attendees will learn about contemporary innovations to both old and new security feature technologies, and design strategies, in use in contemporary security documents. Second, attendees will understand how innovations in genuine document manufacturing affect counterfeiter perceptions, counterfeiter imaging and printing workflows, counterfeiting costs, and how and where counterfeiters can be forced to compromise on counterfeit quality and manufacturability. Virtual hands-on exercises will be facilitated by attendees examining their own personal passports, driver's licenses, birth records, and other security documents.

Counterfeit, Printing, Fraud