Libor Šustr – Technical Director, Optaglio

Dr. Petr Hampl – Security Consultant, Optaglio

THE LATEST TRENDS IN ANTI-COUNTERFEIT PROTECTION FOR CARDS

When it comes to discussing anti-counterfeit protection, it's best to divide the card market into three groups.

Passports, ID cards, driving licenses and other government-issued documents are often targeted by counterfeiters, fueling a continuous race between counterfeiters and protection technology vendors. Counterfeiters should beware, however, that the card industry is very innovative and card issuers are ready to invest considerable resources into security measures.

Employee cards, tickets and membership cards also need anti-counterfeit protection. There is a broad range of applications for these cards, everything from nuclear power plant employee cards to cinema discount cards. Accordingly, different levels of protection are applied. However, there is a general tendency toward adding more and more security elements to these types of cards. This trend is driven by the growing number of security incidents that are not being communicated outside of the companies where they are happening.

Payment cards are simply being looked at as chip holders. Merchants have gotten used to not looking at them at all. Often, a man is allowed to pay with a card that has a woman's name on it and vice versa. With such a high potential for fraud, a fundamental question emerges. If the card is not a real authentication tool, does it make sense to use it? Perhaps it should be replaced by a smartphone payment application? For the payment card to be seen as a real authentication device, it must be protected.

Anti-counterfeit protection technologies designed for one of these card groups can later be applied to protect the other groups. For example, techniques used for protecting passports become outdated. In many cases, these slightly outdated technologies become quite cheap and can be used to provide anti-counterfeit protection for other cards, such as club memberships or library cards. While counterfeiters may be able to learn how to overcome some of the more outdated technologies, they still create additional costs for counterfeiters.

Anti-counterfeit protection should take into consideration both cards and people. While successful counterfeiting could mean creating an exact replica of a card, a fake card can only be successful if the person inspecting the card doesn't see the difference. Therefore, anti-counterfeit protection elements must ensure:

- Imitation is either impossible or extremely expensive.
- The person inspecting the card can determine if it is genuine without the need for special skills.

Polycarbonate, a main topic in the June issue of *Card Manufacturing* magazine, is likely to prevail as a card substrate. It has already become the standard for passport and ID cards, mainly due to its security-based multilayer architecture. Nevertheless, the use of other technologies as composites and improved PVC are emerging. It is also important to note that cards made from economic plastics also need protection because polycarbonate is still relatively expensive.

Cards need to be protected against four basic types of attacks:

- Counterfeiters producing cards with security element imitations.
- Counterfeiters removing security elements from stolen cards and applying them to fake cards.
- Counterfeiters tampering with personalization data on a card.
- Thieves using stolen cards.

People inspecting cards can prevent these counterfeiting attacks with:

- Optical checks
- Machine readers
- Forensics

Card manufacturers continue to add more and more security elements to cards based on a logical assumption that each additional security feature raises the cost of counterfeiting a card. On the other hand, too many security elements can confuse the person inspecting the card. Anti-counterfeit solutions have to take into consideration the skill level of those inspecting the card. Currently, the best-protected cards have about 20 different security elements. Of these, three to five are critical as card inspectors

continued on page 16