STATEMENT OF
MICHAEL H. TERZICH
SENIOR VICE PRESIDENT, GLOBAL SALES AND MARKETING
ZEBRA TECHNOLOGIES CORPORATION

BEFORE THE SUBCOMMITTEE ON HEALTH
COMMITTEE ON ENERGY & COMMERCE
U.S. HOUSE OF REPRESENTATIVES

ON “EXAMINING OPTIONS TO COMBAT HEALTH CARE
WASTE, FRAUD AND ABUSE”

WEDNESDAY, NOVEMBER 28, 2012

Statement Highlights

- Secure ID technology can help significantly reduce the fraud, waste and abuse within the health care system and, more specifically, the Medicare program. It will also aid Medicare by reducing the transaction costs associated with managing the program.
- The Federal Information Processing Standard Publication 201 (FIPS 201) provides a tested framework for bringing secure identity management technology into the fight against health care and Medicare fraud. Leveraging existing FIPS 201 standards will help ensure that the pilot is secure, easy to rollout and adopted by both beneficiaries and providers.
- Counterfeiting secure ID cards is exponentially more difficult than counterfeiting paper-based cards. This enhanced security comes from a combination of media features, printer capabilities, encoding of encrypted data on to the smart chip, database verification and secure methods and processes.
- Both security and efficiency are substantially enhanced through the use of a decentralized print model which provides a concurrent, real-time tie between the creation of a secure ID card and the immediate verification of the cardholder’s information.

Full Statement

Introduction

Thank you, Mr. Chairman, Ranking Member Pallone and members of the Subcommittee. My name is Michael Terzich and I am the Senior Vice President of Global Sales and Marketing for Zebra Technologies Corporation, which is headquartered outside of Chicago in Lincolnshire, Illinois.

I greatly appreciate the opportunity to testify today and share my company's perspective on how secure ID card technology can help address the problem of fraud, waste and abuse in the health care system and, more specifically, the Medicare program.

My company commends you, Mr. Chairman, along with Ranking Member Pallone, for your leadership on this issue. We likewise wish to express our appreciation to your colleague from our home state of Illinois, Congressman John Shimkus, who has worked diligently on this issue and has been a key leader in efforts to eliminate health care and Medicare fraud.

As a global leader in the secure ID digital printer industry, Zebra designs and manufactures a variety of products that use sophisticated technology to safeguard identity and streamline business processes. As a result, I will focus my remarks on H.R. 2925, the Medicare Common Access Card Act, which, as you know, would establish a pilot program to test the potential security benefits associated with modernizing Medicare through the use of secure ID card technology.

Zebra believes that this kind of technology will help protect the continued integrity of the Medicare program. Our confidence reflects the fact that the technology enjoys a strong record of performance in both the federal government and the private sector. From the Department of Defense's use of secure identity credentials for logical and physical access to vital defense facilities and data networks to the work of global credit card companies in advancing combined chip and PIN systems which protect the integrity of both personal identity and financial transactions, secure ID technology provides a tested platform that Medicare can leverage in advancing efforts to combat fraud, waste and abuse.

Moreover, our experience in the private sector is that the digitization of business processes within Medicare will also help reduce the overall cost of operating the Medicare system. On this point, we associate ourselves with the testimony from our colleagues in the Secure ID Coalition, who address this point in greater detail in their statement.

Overall System Benefits

Zebra's products are used by governments and businesses to change processes, making them faster, easier, and more secure. Even the most dedicated employees may eventually err over long periods of time when processing multiple routine transactions. Automating the most mundane, data-centric portions of those tasks allows those employees to focus on the most important aspects of their job, while facilitating the collection of more data, more accurately, with more security. Our experience underscores that substantial cost savings result from this improved accuracy and further opportunities for improvement will arise as data for analysis is more readily available.

Consequently, we believe there will be substantial cost savings for Medicare arising from the use of secure ID technology – both through its ability to combat the waste, fraud and abuse within the current, paper-based Medicare card system and from the efficiencies and savings that will be gained through the digitalization of business processes within the Medicare system. Furthermore, additional savings will be garnered through the ability of secure ID card technology to reduce the incidence of identity theft from recipients and, thus, any consequential issues impacting Medicare personnel due to responding to beneficiaries, reissuing cards or investigating incidents.

As noted previously, we associate ourselves with the testimony of the Secure ID Coalition and understand that the Coalition's statement to the Subcommittee will address the issue of systemic cost savings issue in greater detail. Capturing all such savings takes on even greater urgency as Congress looks to balance the important public policy goals of reducing the deficit and providing health care to our nation's elderly.

Secure Credentialing has Strict Requirements

Secure identity management and verification starts with trusted credentialing technologies. Over the past decade, the federal government has made considerable progress in improving identity security. This experience positions Medicare to leverage the federal government's substantial investment in secure ID technology in the fight against Medicare fraud. This also enhances the effectiveness of back-end analytic tools and will enable enforcement efforts to be more specifically targeted to situations which data analysis indicates merit more thorough investigation.

One of the keystones in the effort to create trusted credentials in the federal government began on August 27, 2004, when then-President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12). Created initially in response to terrorist threats, HSPD-12 directed the use of a common identification credential for both government employees and contractors that would govern both logical and physical access to federally-controlled facilities and information systems.[1]

Following this, the National Institute of Standards and Technology (NIST) created the Federal Information Processing Standard Publication 201 (FIPS 201) for secure and reliable forms of identification. The FIPS 201 requirement for physical and logical access for federal employees and contractors is defined by two stringent standards: Personal Identity Verification I and

[1] Homeland Security Presidential Directive/HSPD-12, Office of the Press Secretary, August 27, 2004. http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html.

Personal Identity Verification II (PIV I and PIV II).[2] The PIV I and PIV II standards affect all secure ID cards designed for use in federal applications and require federal agencies to[3]:

- "Establish roles to facilitate identity proofing, information capture and storage, and card issuance and maintenance."
- "Develop and implement a physical security and information security infrastructure to support these new credentials."
- "Establish processes to support the implementation of a PIV program".

In addition to and following the creation of PIV I and PIV II, NIST created PIV-Interoperable (PIV-I) for use by other organizations that wish to issue secure credentials that are interoperable with the federal government standards.

Deployment of PIV continues to gain momentum. In fact, the federal government has issued millions of FIPS 201 standard PIV cards to federal employees and contractors since 2005 across a wide range of trusted identity applications.[4] Given the federal government's significant and

[2] The PIV I requirements define the control objectives and security requirements described in FIPS 201, including the standard background investigation required for all federal employees and long-term contractors. The PIV II standards define the technical interoperability requirements described in FIPS 201. More specifically, PIV II details the hardware implementation standards for implementing the identity credentials.

[3] "Privacy Impact Assessment for the Department of Justice Personal Identity Verification (PIV) Card System," U.S. Department of Justice, July 20, 2007.

[4] "Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses," Smart Card Alliance, February 2011.

positive experience in using PIV-based secure ID technology elsewhere, we believe it makes sense to employ the FIPS 201 standards in the pilot program that is created by H.R. 2925. Using the current FIPS 201 standards will ensure security, simplify implementation, reduce costs and leverage both the experience and know-how of an existing industry and the federal government's significant investment in the existing infrastructure. As noted previously, the use of FIPS 201 PIV standards will likewise enhance anti-fraud enforcement activities as back-end analytics will be able to more precisely focus on areas of potential concern.

The Importance of Secure ID Card Printers

Counterfeiting secure cards is exponentially more difficult than counterfeiting paper-based cards, even for the most sophisticated, well-financed criminal enterprises. Even if a criminal enterprise could gain access to a secure card printer, it would still have to reverse engineer the security system, obtain secure printing supplies, hack into the secure network, encode PIN or biometric data on the smart chip, print counterfeit cards and then use those cards to create fraudulent transactions – with all of that having to be done before the secure card printer was declared as missing. Even then, each fraudulent transaction would have a known identity which would speed the identification and investigation of subsequent transactions, making it more likely to capture the perpetrators quickly.

Overall, card security comes from a combination of media features, printer capabilities, database verification with encrypted data on the smart chip and secure methods and processes. To prevent counterfeiting, alteration or duplication, there are many techniques that can be used with digital printers. Images or information content can be printed on the card, stored in the chip on the card, or sent to a secure database. When using the information, the combination of data is checked to ensure authenticity.

Even if one of those datasets is compromised, the combination will be known to be invalid and a potential fraud can be more quickly identified. Furthermore, cards with pre-printed security features, including ultraviolet-visible text and graphics or unique on-demand printing capabilities, such as nano-taggant inks or laminate with holographic metallization, can be employed to make counterfeiting more difficult and to create multiple layers of security that allow providers, staff, investigators and law enforcement to identify counterfeit cards. H.R. 2925's pilot program will provide an opportunity to test these features and determine the best combination for the Medicare system.

A Decentralized, Print Model Is Essential

The pilot program contemplated by H.R. 2925 should include and reflect a decentralized print model as a way of further enhancing identity security. The advantages of a decentralized approach reflect the fact that security is enhanced when there is a concurrent, real-time tie between the creation of a secure ID card and the immediate verification of the cardholder's information. Delays or gaps in time between these two steps – which inevitably occur when cards are manufactured in a remote, centralized manner – increase opportunities for fraud that can be otherwise reduced through the use of a decentralized print model.

Consequently, we urge that the pilot program focus on using a model of real-time production of secure ID cards that concurrently verifies a patient's or provider's identity and qualifying status. This will enhance personal accountability and streamline processing, allowing Medicare officials to focus on accuracy and security rather than unproductive processing steps. It will also reduce opportunities for criminals to divert or intercept the card or any corresponding identification documents. By leveraging well-established authentication processes, card security standards, and secure data processing networks, this important enrollment process can be implemented quickly and securely.

Conclusion

When used in a properly implemented system, secure ID card technology enables the use of tested security features which enhance privacy and identity protection. PIV-compliant secure ID cards provide secure, multi-factor authentication at a high level of assurance by combining a cryptographic private authentication with a personal identification number in a durable, tamper-resistant card format. Once a secure ID card is programmed and associated with a user, it provides a trusted, authenticable identity usable for a wide range of cyber-based and physical transactions.

Thank you, again, Mr. Chairman, for the opportunity to testify today. We stand ready to assist the Subcommittee in developing legislative language related to the technical issues I have mentioned and urge the Subcommittee to report out H.R. 2925, with modifications, early next year. I look forward to any questions you or your colleagues may have.