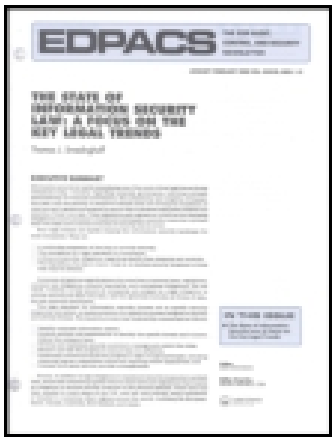

EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

Information Security and Audit Implications of Electronic Money

Slemo Warigon [a]

[a] A Senior Auditor at the University of California in Santa Barbara. He holds a dual B.S. in Computer Information Systems and Accounting from Gallaudet University in Washington, D.C., and an M.B.A. with a special emphasis in General Business and Systems Management from Texas A&M University at Commerce. Warigon has written extensively on various aspects of IS control and security. He is the administrator of the AUDIT-L (General Audit), INFSEC-L (Information Security) and CAATT-L (Computer Assisted Audit Tools and Techniques) Internet discussion lists.

Published online: 21 Dec 2006.

To cite this article: Slemo Warigon (1999) Information Security and Audit Implications of Electronic Money, EDPACS: The EDP Audit, Control, and Security Newsletter, 26:7, 12-15, DOI: 10.1201/1079/43244.26.7.19990101/30237.3

To link to this article: http://dx.doi.org/10.1201/1079/43244.26.7.19990101/30237.3

Felix Pomeranz, Ph.D., CPA is a professor and Associate Director of the School of Accounting at Florida International University in Miami. A retired partner of PriceWaterhouseCoopers, he has authored or co-authored five books and over 100 articles. His article, "Time for Decision on International Accounting Standards," appeared in the November EDPACS.

INFORMATION SECURITY AND AUDIT IMPLICATIONS OF ELECTRONIC MONEY

SLEMO WARIGON

This is the second of two articles dealing with the technology and use of electronic cash. The first article addressed the commercial, privacy, regulatory, and IS security issues associated with the use of electronic cash. The article defined electronic cash as a software-based form of electronic money. Electronic cash was described, further, as the digital equivalent of paper money or currency. It is intended to substitute easily for conventional forms of money in online transactions that include digital coins, electronic checks, and secure electronic credit cards.

The discussion in the first article explained how electronic cash works and is used, assessed the IS security and control features of the use of digital and blind signature technology to authenticate cash transactions, summarized the offerings of six major electronic cash purveyors, and examined the commercial, personal privacy, and regulatory implications of electronic cash. Particular attention was given in the first article to the current government stances toward the evolution of electronic cash mechanisms. It was noted that, in general, the U.S. government has adopted a wait-and-see attitude about the regulation of these mechanisms. Among the issues that will need to be resolved, eventually, are taxation, money laundering, and customer protection in Cyberspace.

Security is, perhaps, the most critical aspect of electronic cash. It is where the IS audit and control professional can play a positive role in bringing about economic change.

REVIEW APPROACH

Privacy laws may place legislated restrictions on the collection and retention of audit trails by electronic cash security features, or application logging facilities. This could inhibit control specialists from performing postcontrol reviews of electronic transactions. Without such legislated restrictions,

postcontrol review may be conducted on a limited basis mainly to determine whether controls worked as they should, and to use historical electronic data for various purposes (such as trend analysis, forecasting, and marketing).

Strategic Advantages

Use of organizational electronic cash mechanisms will create detailed information about the financial activities of an enterprise. Electronic cash transactions may make up the bulk of information assets that are critical to the survival of an organization in an increasingly competitive environment. These assets will be vulnerable to industrial espionage by competitors, the mass media, class action litigators, environmental groups, and international terrorists.

IS audit and control specialists might be called upon to assist their organizations in quantifying the value of such information, determining the acceptable levels of security for the information, and proposing appropriate defensive security measures to counter such things as industrial espionage activities.

Also, IS audit and control specialists may recommend the widespread use of electronic cash mechanisms in their organizations to exploit these strategic advantages:

- *Fraud deterrence:* programming the use of organizational electronic cash for specific purposes. The use of the system can be restricted, for example, to a specific location, to a specific timeframe, to the purchase of specific authorized materials and services, and to approved users only.
- *Flexibility:* an organization can use electronic cash for both small and large purchases conveniently and securely in a paperless environment.
- *Cost savings:* processing electronic cash transactions will be considerably less expensive than handling traditional payment methods, such as cash, checks, and credit cards. The use of electronic cash will reduce the number of employees required to handle traditional payment methods, and the control procedures that are associated with these mechanisms.
- *Speed:* electronic cash transactions will be accomplished at the speed of light. A delayed processing of payment, a bounced check, or a declined credit card transaction will be a thing of the past.
- *Proactivity:* the use of electronic cash will encourage enterprises to embrace a culture of proactivity, rather than continuing to operate in a crisis mode.

PROCESSING ELECTRONIC CASH TRANSACTIONS WILL BE CONSIDERABLY LESS EXPENSIVE THAN HANDLING TRADITIONAL PAYMENT METHODS.

CREATING NEW OPPORTUNITIES

Electronic cash is expected to create new opportunities and to break down barriers to the spread of electronic commerce. It will revolutionize the way in which money is perceived and used. Also, electronic cash will transform the way in which individuals and organizations manage money. Immense benefits can be reaped from widespread use of electronic cash. Also, its

extensive use will present new and complex challenges to control-oriented professionals. To meet these emerging challenges better and to provide added value to their organizations, these professionals will need to shift the gear of their control vehicle from a primarily detective mode (that is, reactive approaches) to a primarily preventive mode (that is, proactive approaches).

New opportunities in the volatile electronic cash industry present new risks. Those enterprises that enter the developing electronic cash industry will face a classic marketing dilemma: stay conservative or be aggressive. Conservative organizations may end up abdicating the bulk of a flourishing environment to their competitors. In contrast, aggressive organizations will expand vigorously to take full advantage of the new opportunities, even if it means cutting some corners as they seek to grow.

ALLOWING DIVERSE ELECTRONIC CASH BRANDS TO EVOLVE WITHOUT PREMATURE GOVERNMENT INVOLVEMENT MAY BE UNREALISTIC.

The assertion that the public interest will be best served by allowing diverse electronic cash brands to evolve without premature government involvement may be unrealistic. Any attempt to apply the doctrine of laissez faire slavishly in a volatile industry is doomed, probably, from the outset. Allowing individual competitors with divergent agendas to make important public-policy decisions without a coherent, visionary plan of action by a proactive government may be costly and ineffective. The transition to a cashless society may not be orderly.

This may call for an early involvement of governments with the political will to manage an orderly transition to a cashless economy in a manner that maximizes quality outcomes for all parties concerned. Such involvement may not necessarily stifle competition and innovations in the marketplace. It could entail making policy decisions on the social and economic issues associated with electronic cash technologies. And it may entail such actions as mandating a central entity to issue a basic control framework (that is, a set of standards) that should be followed by all entities in the electronic cash marketplace.

Unconstrained Standards

Ideally, the electronic cash standards and guidelines do not need to be constrained by national ideologies or cultural ethnocentrism. Standards and guidelines will need to embrace more global issues, such as access controls, contingency planning, legal requirements for electronic evidence, and product quality and performance warranties. Global acceptance of electronic cash standards and guidelines issued by an internationally recognized central body may make uniform compliance feasible.

IS audit and control professionals from various countries will need to get involved in this standard-setting process to ensure that fundamental control issues are addressed properly. Many of the principles which undergird quality-oriented strategic planning can assist in the formulation of electronic cash standards and guidelines. These principles focus on these categories:

- *Philosophy:* stress focus on consumer needs in a never-ending search for quality.
- *Social environment:* establish norms and values that dictate the proper treatment of each individual in an organization or society.
- *Process:* stress the need for problem prevention throughout the planning process, rather than the identification of failures at the end of the process. Finally, the stakes in the developing electronic cash industry are too high to allow anyone to be a mere spectator.

The survival motto in the digital age is: Not reacting to change, but leading it! ■

Slemo Warigon, CISA, is a Senior Auditor at the University of California in Santa Barbara. He holds a dual B.S. in Computer Information Systems and Accounting from Gallaudet University in Washington, D.C., and an M.B.A. with a special emphasis in General Business and Systems Management from Texas A&M University at Commerce. Warigon has written extensively on various aspects of IS control and security. He is the administrator of the AUDIT-L (General Audit), INFSEC-L (Information Security) and CAATT-L (Computer Assisted Audit Tools and Techniques) Internet discussion lists.

TWO IMPORTANT DATA ENCRYPTION STRUCTURES REPORTED BROKEN IN RECORD TIMES

BELDEN MENKUS

Paul Kocher, John Gilmore, and their associates in the San Francisco-based Cryptography Research reportedly decrypted two important data encryption structures in what was described in each instance as record-setting times. One is the *U.S. Data Encryption Standard*, or DES, used widely in numerous unclassified U.S. government agency and banking industry funds storage and transfer and other highly sensitive information-processing applications. The other is the data encryption mechanism that is used in the latest generation of so-called *smart cards*.

THE U.S. DATA ENCRYPTION STANDARD

As Tony Patti pointed out in the August 1993 issue of *EDPACS*, the DES is an outgrowth of 1968 information-processing technology. Its basic complexity, and thus, its *cryptographic strength,* is a reflection of the relative computing speed and technology sophistication of that period. (The