Assessment of Threats for Smart Card based Electronic Cash

Kazuo J. Ezawa
Gregory Napiorkowski

Mondex International Limited
Atlantic Technology Center
Suite 109
100 Campus Drive
P.O. Box 972
Florham Park, New Jersey, 07932-0972
USA

Abstract. The security of smart card based electronic cash have been receiving significant attention recently. However, there has been little systematic analysis or quantification of the impact of the security break on the smart card based electronic cash economy. This paper discusses the assessment of threats in two phases using two different methodologies. The first is the assessment of overall threat using the business system analysis model called "value chain" - the methodology to evaluate the activities necessary to achieve the final objectives of the counterfeiting organization. It is a qualitative method. The second is the quantification of such a threat using micro dynamic simulation.

1 Introduction

There have been many technical discussions of the security of smart card based electronic cash. However, there has been little attention paid to the systematic analysis of the way to achieve objectives of counterfeiting (e.g., economic gain, sabotage, blackmail, etc.), nor the subsequent quantification of the impact of the security break on the smart card based electronic cash economy. Clearly, one has to perform these analyses before one claims the demise of the smart card based electronic cash. This paper discusses the assessment of threats in two phases using two different methodologies. The first phase is the assessment of overall threat using the business system analysis model called "value chain" [5] - the methodology to evaluate the activities necessary to achieve the final objectives of the counterfeiting organization. It is a qualitative method. The second phase is the quantification of such a threat using micro dynamic simulation.

The counterfeiter's challenges are both strictly technical as well as of organizational and behavioral nature, and go well beyond the security break, a formidable barrier itself, but only the first barrier to be broken. This paper discusses how a global smart card based electronic cash product (such as Mondex electronic cash) using various security, risk management capability, and taking advantages of other natural human and organizational behaviors prevents counterfeiters from achieving their ultimate goal.

The paper is organized as follows. Section 1 describes the qualitative assessment using the counterfeiter’s value chain model. It discusses using two illustrative examples overall challenges that are faced by the counterfeiters. Section 2 discusses the quantification of impact of counterfeiter’s threat scenarios using micro dynamic simulator. Section 3 summarizes the discussion.

2 Qualitative Overall Assessment of Threats using Business System Analysis Methodology

There are many possible motivations for counterfeiting smart card based electronic cash application; from the economic gain, to fame, to sabotage, and to the international blackmail. Whatever the motive of the counterfeiter, it is beneficial to analyze the counterfeiter’s “*value chain*”[1] from the business perspective, since the principal motivation for setting up a counterfeiting operation is to achieve an “objective.” Clearly, depending on the objectives, types of the target product for the counterfeiting, and types of exploitation strategies (threat scenarios), the value chain model will look different.

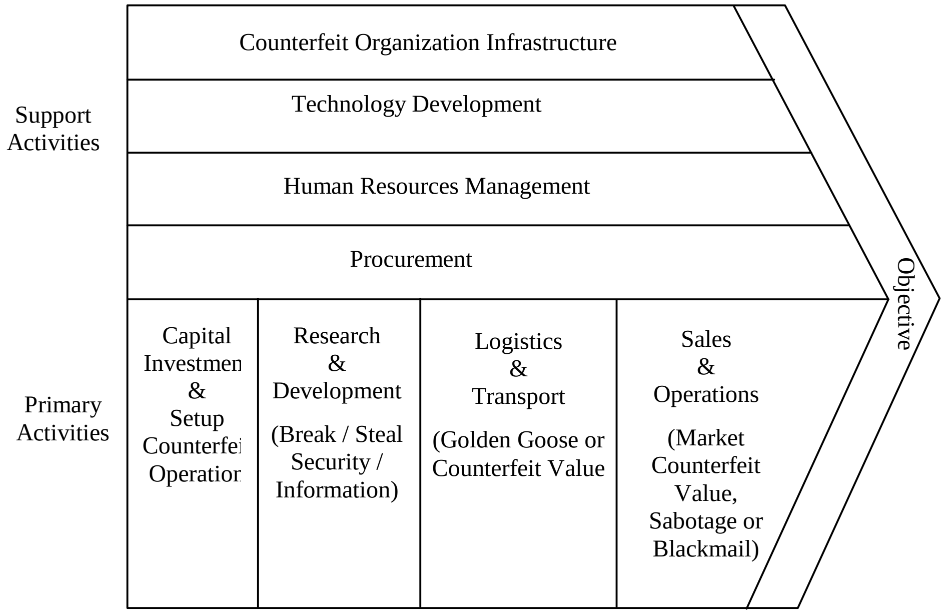

Counterfeit Organization Infrastructure
Technology Development
Human Resources Management
Procurement
Support Activities
Primary Activities
Capital Investmen & Setup Counterfei Operatior
Research & Development (Break / Steal Security / Information)
Logistics & Transport (Golden Goose or Counterfeit Value
Sales & Operations (Market Counterfeit Value, Sabotage or Blackmail)
Objective

Figure 1. Generic Counterfeiter’s Value Chain

[1] The business system concept of value chain captures the idea that a firm or, in our case, a counterfeit organization has a series of functions to perform, and each of them needs to accomplish some specific goals in order to produce a profit.

The value chain model explicitly and visually describes the requirement for the supporting infrastructure and the primary activities of the organization to accomplish the mission. The model is a *qualitative model*, and has been extensively used in the business to evaluate the effectiveness of the firm and the competitive position in the industry that it serves. In this paper, we explore the value chain models that assume one of the possible motivations - "profit generation" as the primary objective of the organization to counterfeit smart card based electronic cash application[2]. Each threat scenario has its unique resource, organizational and primary activities requirement. Therefore the value chain model and its associated analysis is different for each threat scenario.

Once the model identifies strength and weakness of the firm, further *quantitative analysis* is conducted to gain additional insights and recommendations to improve the firm's competitive position in the industry. The use of micro dynamic simulation for the quantification of counterfeit threat scenarios is discussed in the section 2.

The counterfeit organization requires a good "business case" before it commits the substantial up-front investment, large organizational resources and time to a "project". It is logical for such an organization to evaluate its counterfeiting business, as one of many business opportunities, in terms of return on investment. The business case for counterfeiting has to be superior to its alternatives.

Figure 1 shows the generic counterfeiter's value chain. There are two types of activities: support and primary. The support activities include the organization's infrastructure (e.g., network of agents, offices, etc.), technology development (e.g., technology to break the security barriers), human resource management (i.e., assembling various technical skilled and operational skilled personnel), and procurement (i.e., hardware, software, and others). The primary activities show a chain of tasks required to achieve an objective of the organization. They include, the capital investment and setting up of the counterfeit operations, the research and development (i.e., breaking the security or stealing security information), the logistics and transportation of counterfeited application (i.e., golden goose) or counterfeit values, and the sales and operations (i.e., marketing of counterfeit value or blackmail.)

In the following section, we discuss the global smart card based electronic cash product features. Some of the features are designed so that they make the counterfeiter's challenges to be formidable. After the discussion of product features, two counterfeit scenarios are examined using value chain models. One is the street corner counterfeit value distribution scenario, and the other is the case when a member (bank) is the catalyst for the counterfeit activities.

2.1 Global Smart Card Based Electronic Cash Product

[2] There are many other non-profit oriented attack scenarios with objectives such as "just for fun" (e.g., by university students), fame, or political blackmail by foreign government. They constitute important threat scenarios not to be ignored, but for this paper, we discuss only the two specific scenarios with "profit" motivation.

The global smart card based electronic cash product such as Mondex electronic cash has the security and the risk management to prevent, detect, contain, and recover from potential counterfeit activities. It is designed to make counterfeiter's "chain" of tasks as difficult as possible in every step of the way.

The product is designed for the efficient electronic cash payment transactions. It performs purse (chip) to purse (chip) transactions without central authorization. It has many on-chip capability and features such as physical security, cryptographic security, purse class structure (i.e., it restrict the interactions of different type of purses), purse limit, on-chip risk management capability (e.g., credit turnover limit), and migration[3]. Security issues related to Mondex electronic cash application are discussed in [4]. Purse class structure, purse limit, credit turnover limit will be revisited in the following section.

Figure 2 shows the Mondex transactions among the different classes of purses. Solid line indicates transactions currently allowed, and dotted line indicates the transactions severely restricted (or disallowed) at this stage of product evolution.

Ideally, an advanced smart card based electronic cash scheme, as a substitute for "real" money, should parallel the existing money supply and banking system. Therefore such a scheme would include a currency "originator" (equivalent of central bank), and "members" (commercial banks and other financial institutions with their branches). There are merchants who transact with consumers and members, and consumers transacting with other consumers, merchants, and members.

In the following we discuss non-security related features:

Chip to Chip: The value (electronic cash) is transferred from payer purse (chip) to payee purse (chip) without third party authorization. Even if a counterfeiter succeeds in creating a "golden goose", it has to transact with other legitimate purses to actually transfer counterfeit value. The transacting purse has on-chip risk management capability to monitor "unusual" behavior of the purse transaction pattern.

Purse Class Structure: It classifies purses into different types of purses and determines what types of purses can transact with each other. Each purse can transact only with predetermined list of purse classes. For example, a consumer purse which is linked to the purse holder's direct deposit account of the member can transact with other consumer purses, two types of member purses, and three types of merchant purses.

Purse limits: High value limit purses (such as originator, and member purses) are monitored on line. All transactions to and from these purses are recorded and monitored (e.g., merchants and consumer deposit transactions.) Consumer purses are expected to have relatively low purse limits (e.g., up to $1000.)

[3] It involves switching of one public key scheme to the other.

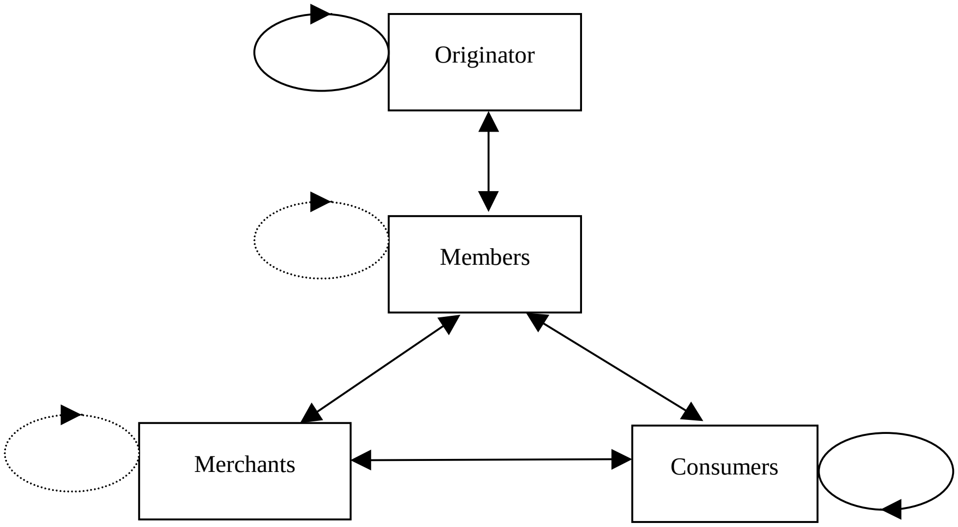


Figure 2. Transactions among different class of purses

Credit turnover limit: An on-chip risk management capability to monitor amount of value being received by a consumer purse from non-member purses such as consumer to consumer, and merchant refund transactions. If the transaction causes the credit turnover limit to be exceeded, this on-chip logic suspends a part or whole features of the purse. The credit turnover limit is customized by members to fit for the purse holder's normal needs.

One of the critical elements and advantages of the on-chip risk management capability (such as credit turnover limit) is that it continuously functions on the legitimate purses and constrain the flow of counterfeit value, even under complete physical security breakdown of the attacked purses. The fact that the risk management functionality of the compromised chip will be disabled doesn't directly benefit the counterfeiters. They need to interact with legitimate purses (cards) which still have active and functioning on-chip risk management capability. It is unlikely to be able to transfer all the counterfeit value to legitimate purses without triggering some actions by this on-chip risk management capability/logic.

In what follows, the two cases of counterfeit scenarios mentioned earlier are examined using value chain models. Case 1 covers the threat scenario when the counterfeit value is distributed through the personal contacts with the potential buyers – "street corner counterfeit value distribution." Case 2 examines the threat scenario when a member bank is owned by the criminal organization, and it is used to distribute the counterfeit value.

2.2 Case 1: Examination of Primary Activities of Counterfeiter's Value Chain of the Street Corner Counterfeit Value Distribution Threat Scenario

There are a few ways to obtain economic gains from the counterfeit value. We discuss only a few just to illustrate the counterfeiter's challenges. One way is to purchase goods and services, which imposes physical constraints on the return of counterfeit investment, and logistic problems (e.g., transporting goods.) Alternatively, agents can deposit the counterfeit value into the financial institutions. Both approaches require agents to reveal themselves either face to face or on-line.

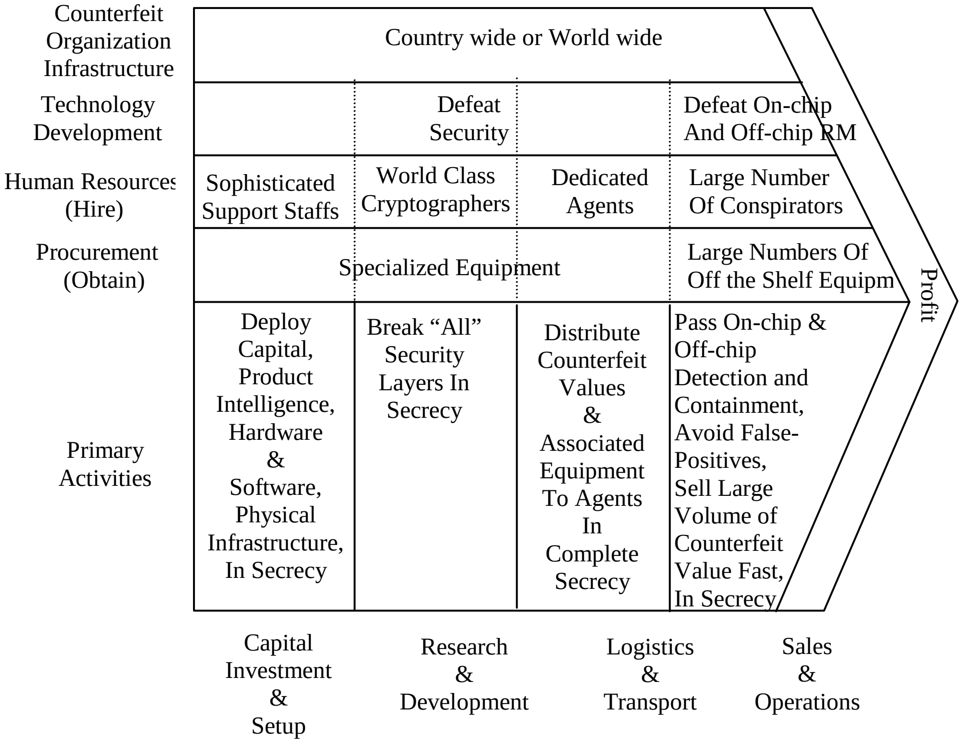
Another approach is to sell, at a discount, counterfeit electronic cash to a fraudulent population, in exchange for "real" local currency. The fraudulent population is defined as the one that would engage in such transactions knowingly and willingly. The fraudulent population is not necessarily as loyal as agents of counterfeit organization and the "secret" is bound to be leaked to the law enforcement institutions or electronic cash issuing institution.

Figure 3 shows the counterfeiter's value chain for this scenario. Vertical items on the left of the chain show organizational functions of both primary and support activities. Horizontal items represent a series of objectives that need to be accomplished to produce a profit.

As the counterfeiter's value chain shows, due to the product features (as described in the next section), it requires some formidable organization and resources, up front capital investment, and flawless executions of technical as well as operational tasks against determined foes (various authorities and electronic cash organizations such as Mondex) to make a financial gain. Another prerequisite for a business success is a well financed, functioning, controlled, and coordinated organization with extremely loyal followers. Moreover, it needs people with a variety of technical and operational skills. Some of them have to be world class experts in various fields (e.g. cryptography). Finally, one has to establish a country wide or even world wide network to be able to "cash in" large amounts of counterfeit values in a very short time before the incidence responses are triggered by the electronic cash operators.

The following illustrates some activities that have to be successfully carried out.

Security break (in research & development): This task, difficult by itself, requires an access to or purchase of very specialized equipment. Moreover, a complete secrecy has to be maintained over an extended period of time while various tasks are performed to break security. A success requires not only cryptographic or physical break, but other layers of security measures would have to be compromised as well.



	Capital Investment & Setup	Research & Development	Logistics & Transport	Sales & Operations
Counterfeit Organization Infrastructure	Country wide or World wide			
Technology Development		Defeat Security		Defeat On-chip And Off-chip RM
Human Resources (Hire)	Sophisticated Support Staffs	World Class Cryptographers	Dedicated Agents	Large Number Of Conspirators
Procurement (Obtain)	Specialized Equipment			Large Numbers Of Off the Shelf Equipm
Primary Activities	Deploy Capital, Product Intelligence, Hardware & Software, Physical Infrastructure, In Secrecy	Break "All" Security Layers In Secrecy	Distribute Counterfeit Values & Associated Equipment To Agents In Complete Secrecy	Pass On-chip & Off-chip Detection and Containment, Avoid False-Positives, Sell Large Volume of Counterfeit Value Fast, In Secrecy

Figure 3. Counterfeiter's Value Chain Model
of the Street Corner Counterfeit Value Distribution Threat Scenario

Creation of counterfeit electronic cash application (in research & development): Assume that the security was broken in the lab environment. The next challenge is to create a "shrink wrap" product of "golden goose" that can generate counterfeit electronic cash with flawless imitation of electronic cash application (e.g., Mondex purse) functionality. If the agents use legitimate electronic cash cards such as Mondex purses for their distribution, on-chip risk management feature will quickly pick up and disable these cards[4]. It has to be robust enough to be operated by technically less sophisticated people. One has to pass quality control that wrong operations or malfunctions will not leak the counterfeit activity information to the authorities and/or electronic cash issuing institutions.

Counterfeit value distribution channels (in logistics & transport): It has to solve the logistics. A counterfeiting organization has to be able to distribute "golden goose" or counterfeit values to its agents in complete "security" and secrecy. It takes time to set up secure and trustworthy channels of distribution. The "product" is a very tempting target for "interceptions" by the agents inside as well as outside the

[4] This has been confirmed in the various counterfeit threat scenarios using the Mondex Micro Dynamic Simulator.

organization (such as competing "firm".) And there's always a problem of "informants".

Marketing and sales - false positive problem (in sales & operations): A critical challenge for the counterfeiter/agents is to correctly identify "fraudulent" population whose size is small. If they approach a normal/honest person, he or she might inform the financial institution or authority (statistically speaking, this is called a false positive problem for the counterfeiter.) It is a difficult task to identify a small population, and it's statistically nearly impossible not to have false positives. But the counterfeit organization has to avoid false positives.

Behavioral problem of fraudulent population due to on-chip risk management capability (in sales & operations): Now, even if the false positive problems are solved, there remains a behavioral challenge posed by the fraudulent population. Legitimate electronic cash cards, such as Mondex purse, of the fraudulent population still have active and functioning on-chip risk management on them. It detects unusual flow of values from/to the card, and in some specific cases it disables certain card functionality. As a result, the card owner has to contact the issuing financial institution[5], if she/he wants to bring back this functionality. If the card is linked to the individual's bank account, such a contact is a necessary step to regain access to the bank account, thereby passing the information of potential counterfeit value transactions to the financial institutions. Alternatively, a card owner may choose just to report lost or stolen card, but this very act would trigger some investigation as well. Quantification of impact of this on-chip risk management capability is discussed in section 3. The counterfeiting organization has to solve these fraudulent population's behavioral problems.

Avoidance of off-chip detection (in sales & operations): Then, there is the off-chip (host system based) risk management capability. The counterfeit value bought by the fraudulent population has to be spent to obtain economic gain. Sudden rise in redemption of value can be detected quickly.

Various types of models are used for the detection tasks at various stages and layers of the scheme in the case of Mondex. Mondex risk management philosophy calls not for the adoption of one technology or method, but a balance of different methodologies complementing each other. For example, advanced statistical methods are used in the currency (float) monitoring systems, merchant and consumer monitoring systems, etc. And the Bayesian machine learning method [1,2, and 3] is used for monitoring transactions that are "flagged" by the on-chip risk management. Other complementary detection methods will be used as needed.

[5] Suppose a fraudulent person paid "real" $100 for $300 Mondex counterfeit value and cannot spend the acquired counterfeit value due to the on-chip risk management; such person has an incentive to contact the issuing financial institution for the release of value, or request "money back" from the agent.

The counterfeit value distribution activities have to clear the barriers imposed by these detection models.

Consideration of incidence response (in sales & operations => termination): As illustrated by the credit turnover limit example, some of the on-chip risk management capability contains on-chip incident response mechanism in an autonomous mode. On the other hand, one of the most effective ways to respond to the counterfeit contingency is to activate, by a central command, on-chip incidence response to affect a contaminated segment of purses (cards.) It will then function autonomously without outside intervention. It is the fastest way to respond to a potential incident. It can trigger a various incidence responses, including on-chip incidence response [e.g., migration]. This will stop the cash flow to the counterfeiting organization. Therefore the organization has to gain enough profit before the counterfeit activities are shut down.

In theory, any of the above links in the "from security to risk management" chain can be broken. However, as shown above, it is an extremely difficult task to carry out flawlessly in the real world in every step of the way, and against technological, organizational, and human behavioral challenges. Moreover, the tasks have to be accomplished while facing powerful and determined foes, such as government authorities and the electronic cash institutions. Therefore, it is very unlikely that the business case for counterfeiting be attractive enough to justify the overall investments needed against other alternative "business" opportunities.

2.3 Case 2: Examination of Primary Activities of Counterfeiter's Value Chain of the Member Counterfeit Value Distribution Threat Scenario

Now consider the threat scenario that a member (bank) is involved in the distribution of counterfeit activities. Figure 4 shows the counterfeiter's value chain model of the member counterfeit value distribution threat scenario. There are some critical differences from the Case 1. It assumes that the member bank is distributing counterfeit value to the consumers. It provides a portion of consumer withdrawals with counterfeit values (i.e., skimming strategy) to avoid detection by the originator.

The criminal organization may control a bank to cover its criminal activities. If the bank is owned by the criminal organization, it may perform many of the most critical functions from distribution of financial assets to investment of illegally accumulated fund in the legitimate markets.

Business Case (evaluation to enter counterfeit business): Before a criminal organization commits its bank to the counterfeiting an electronic cash, its business case of counterfeiting has to pass not only the return on the investment criteria of the crime organization, but also the contingency of losing the bank due to the "exposure" through the counterfeit detection and incident response. One has to consider not only the lost investment for the counterfeiting but also the loss of the critical element of the criminal organization, the loss caused by the termination of other criminal activities, and, last but not least, the loss of accumulated financial investments and assets if the bank is seized by the authority. Investments in the Mondex member license and the Mondex infrastructure for the bank are lost as well.

In the following, we discuss some of the activities that have to be successfully carried out by the counterfeiter.

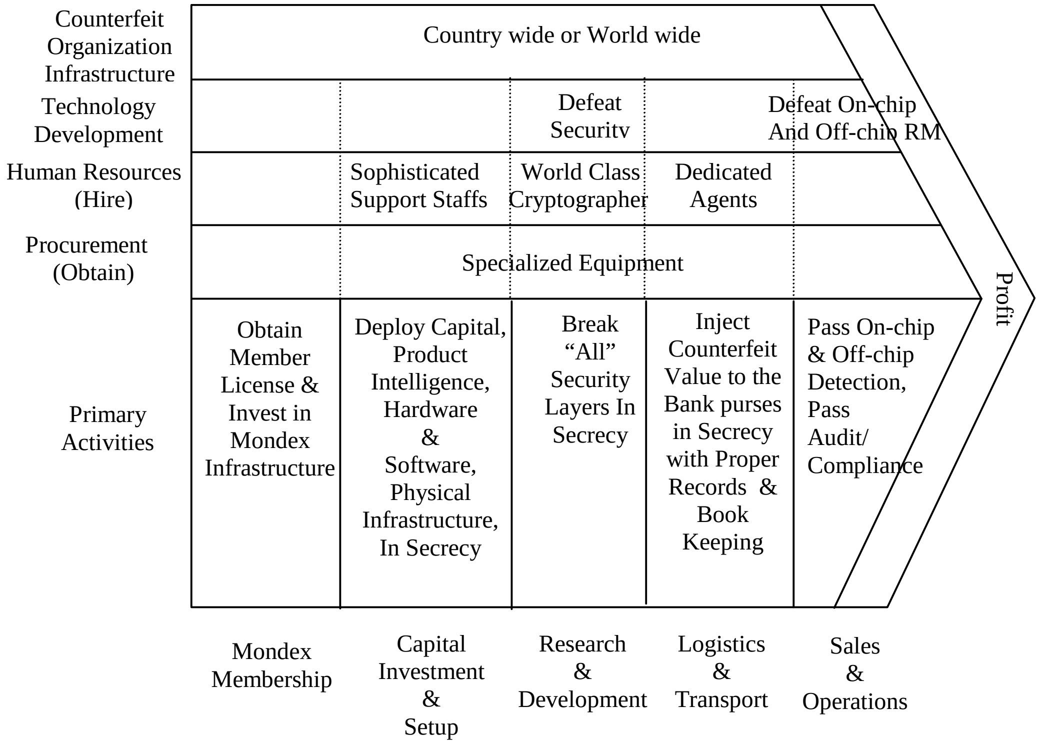

Counterfeit Organization Infrastructure
Technology Development
Human Resources (Hire)
Procurement (Obtain)
Primary Activities
Country wide or World wide
Defeat Securitv
Defeat On-chip And Off-chip RM
Sophisticated Support Staffs
World Class Cryptographer
Dedicated Agents
Specialized Equipment
Obtain Member License & Invest in Mondex Infrastructure
Deploy Capital, Product Intelligence, Hardware & Software, Physical Infrastructure, In Secrecy
Break "All" Security Layers In Secrecy
Inject Counterfeit Value to the Bank purses in Secrecy with Proper Records & Book Keeping
Pass On-chip & Off-chip Detection, Pass Audit/ Compliance
Profit
Mondex Membership
Capital Investment & Setup
Research & Development
Logistics & Transport
Sales & Operations

Figure 4. Counterfeiter's Value Chain Model
of the Member Counterfeit Value Distribution Threat Scenario

*Member License (in Mondex membership)***:** The member has to pass the minimum requirement to qualify for the member license. All critical aspects of the member including internal controls, security, and operations are reviewed carefully by the originator. Although the funds may not directly come from the criminal organization, the bank has to invest in the creation of Mondex infrastructure to provide Mondex services.

Security Break (in research & development): Availability of member purses are limited, their uses are restricted, and carefully monitored on line. Higher value limit purses are stored in the physically secure and restricted area. Note that although the bank is owned by the criminal organization, not all the employees are its agents (different skill sets required to run banks.) Member to member transactions are not permitted. Hence there's no special advantage attributed to counterfeiting member purse which is more difficult to obtain than that of the consumer's. The counterfeiter can create the consumer counterfeit purse and inject the counterfeit value to the member purse directly or indirectly through colluding merchants. The technical difficulty to break the layers of the security is the same as Case 1.

Injection of counterfeit value to the member purse system (in logistics & transport): The scenario assumes that the consumer counterfeit purse is used to inject counterfeit value into the member purse system. The agents have to have access to various physical and data security, and modify associated data transaction records, and accounting (book keeping records.) For the bank to be credible, it has to be run by professionals, have a formal organization, and follow the banking regulations. It has to pass the scrutiny of internal professionals as well. Also, it has to solve the problem of informants. One cannot assume that all bank employees are loyal to the criminal organization.

Counterfeit value distribution (in sales & operations): One way to avoid immediate detection is to use the skimming strategy. That is when a consumer withdraws (buys) Mondex value from the member, the counterfeiter provides a mix of the legitimate and the counterfeit Mondex value. Depending on the size of the bank, an ability to sell counterfeit value through consumers is limited. If the bank has 100,000 consumer purses, and each withdraws $100 per week with 10% counterfeit value, the bank can inject $1 million counterfeit value per week. It takes time to recover the investment of counterfeiting, and if the counterfeiting is found in the bank, all its asset might be confiscated.

Avoidance of on-chip control (in sales & operations): Member purse transactions are controlled by the purse class structure, and purse limit. The value transfers across members are not permitted. The amounts of transfers to consumer or merchant purses are constrained by the respective purse limits. One has to overcome these obstacles.

Avoidance of off-chip detection (in sales & operations): The counterfeiter has to pass the off-chip (host system based) monitoring by the originator that deploys and operates the currency monitoring and the member monitoring systems. Members are the critical focus of monitoring by the originator. Any unusual behaviors are immediately reviewed and inspected. As for detection models, the impact of skimming attacks have been quantified and analyzed using various techniques. Statistical detection models for the skimming threat scenarios have been developed to monitor such attacks. One has to clear these off-chip detection screens.

Passing audit/compliance/inspection (in sales & operations): Every bank is subject to audit, compliance, and inspections by various authorities, and some private organizations including Mondex. It has to pass regular and ad-hoc visits of auditors and other inspectors. The banks that are suspected to be owned by criminal organizations are objects of continuous surveillance by the authorities.

Anticipation of incident response (in sales & operation => termination): Once the counterfeit is detected, on-chip incident response can be invoked to stop the infusion of counterfeit value. Furthermore, even if the counterfeiter may not be captured, but the critical asset, the bank, is left for seizure by the authority. Assets that the counterfeiter has accumulated in the past through various other criminal activities as well as "legitimate" activities would be lost as well. The counterfeiting organization has to generate enough profit before the termination of counterfeit activities, and not to leave a trace to the bank. Note that all the cards issued by the bank have the unique bank identification number that is recorded as a part of transaction log whenever transaction occurs. Hence the value transfer from the bank can be traced.

In summary, considering all the assets the counterfeiter has in the bank put at risk, the relatively moderate counterfeit profit that requires flawlessly execution of all the primary tasks doesn't seem to justify the counterfeiting business case.

3 Quantitative Assessment of Threats using Micro Dynamic Simulation

As we discussed in the previous section of qualitative assessment, once the additional need for the analysis is identified, the quantitative assessment of the threat scenario is performed using various analytical tools. In this section we discuss the use of the simulation model. To quantify a threat scenario, one needs to observe or model, the following phases: 1) Creation of counterfeit value, 2) Interaction of electronic purses (transactions), 3) Diffusion of both legitimate and counterfeit value throughout the economy, and 4) Incident responses (countermeasures).

At the moment, no actual data on the counterfeit activities exist in the new electronic cash economy. Moreover, it is extremely unlikely that any actual observations regarding counterfeit value will be available in the foreseeable future. Therefore a quantification of a given threat scenario has to be based on the observations generated in a laboratory-like environment. Simulation modeling offers such an environment. It allows, through setting distributions of various parameters, to control and observe the behavior of all phases of a threat scenario. Depending on their properties and underlying techniques, different classifications of simulation models can be used. The simulation models can be classified based on the level of aggregation of modeled phenomena and the role played by the "time" variable. According to the first criterion, the simulation models are assigned into *macro* or *micro* categories. The second criterion differentiates the *dynamic* models from the *static* ones. A more comprehensive discussion of these model classes can be found in [5], where a number of static and dynamic micro simulation models to evaluate tax, social and general economic polices are introduced.

The task to quantify a threat scenario requires, among other information, data on individual purses' transactions as well as on the effectiveness of the on-chip based response. Therefore we use the *micro dynamic simulation model*. In general, it is a computer model that imitates the dynamics of the electronic cash scheme. It has the following important features: 1) Mimics the expected longer term evolution of the electronic cash scheme, 2) Reflects, through respective model parameters, short term behavioral patterns, e.g. seasonal fluctuations, 3) Follows the transaction behavior of individual purses, e.g. a number and frequency of transactions, and 4) Keeps a complete record of all individual transactions.

The above features allow an analyst to perform various experiments. The essence of every experiment is to: 1) Design a threat scenario and inject the related counterfeit value into the system, and 2) Build in and invoke during the simulation the on-chip and off-chip based responses.

The simulated diffusion of the counterfeit value and an effectiveness with which it can be detected and contained provide the critical information that allows us to quantify a threat scenario in question.

3.1 Mondex Micro Dynamic Simulator

Mondex Micro Dynamic Simulator (simulator for short) is a particular application of the micro dynamic simulation concept to the Mondex electronic cash scheme. The model's design is flexible enough to reflect not just today's but also other possible future scheme structures. The simulator was used to assess the effectiveness of the selected responses against the likely threats.

The attached appendix shows examples of input and output screens of the simulator. To increase model's flexibility and the level of detail, as far as the transaction patterns are concerned, each level of scheme participants can be further segmented. Segments within the same level of participants differ from each other by their respective transaction patterns, as defined, for instance, by number and type of daily transactions.

Figure 5 in the Appendix shows a window that defines a member segment given the originator. It allows the user to specify various characteristics of the member segment, ranging from, for example, member type (merchant bank, consumer bank, or both) to birth/death rates for members, merchants and consumers (i.e. population growth and decline.) Member segments can be declared as counterfeit segments by clicking the corresponding "counterfeit" check box. Note that, at the purse level, the simulator keeps tracks of individual purse setting such as purse limit, value balance and on-chip risk management functionality.

Figure 6 in the Appendix shows the impact that counterfeit activities have on the number of locked up purses. This is the direct effect of the on-chip risk management functionality. The locked up purses are the legitimate ones that happen to be contacted by the counterfeit purses in order to receive the created counterfeit value. When a preset condition is met, the on-chip risk management functionality turns on on-chip response autonomously in this case locking up the purses.

An ability to produce and analyze multiple runs of the simulator model under different scenarios allows the user to experience the management of the electronic cash economy before the scheme is actually rolled out.

The risk management capabilities need to be continuously upgraded to match new potential threats in the rapidly evolving electronic commerce. The simulator model plays a critical role in the evaluation of both on-chip and off-chip new risk management tools to anticipate and prepare for the future counterfeit challenges.

In addition to being a tool to evaluate the impact of counterfeit scenarios, the simulator model also generates transactions that can be used to train off-chip detection model(s). The simulator model is to be calibrated for every respective currency originator (i.e. country) to reflect the particular behavior of its purse users and their transaction patterns of their territories.

4 Summary

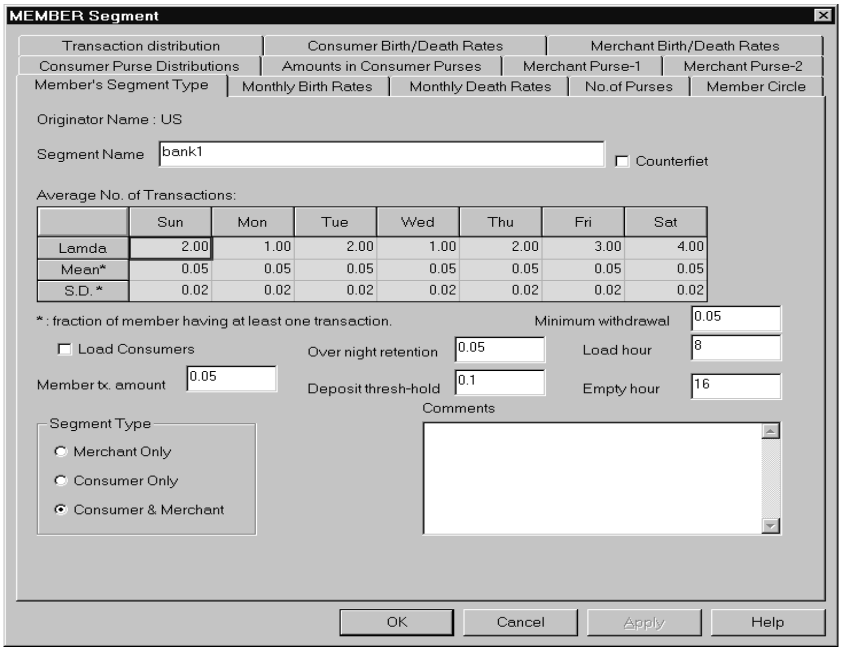
We discussed the qualitative and the quantitative assessment of threats for smart card based electronic cash. In the qualitative assessment section we discussed the counterfeiters' enormous technical as well as organizational / behavioral challenges that go far beyond the security break which itself constitutes a formidable barrier to overcome. The counterfeiting organization's value chain and its associated tasks are examined. We discussed two cases of threat scenarios and concluded that it would be very difficult to justify a "business case" for undertaking counterfeiting activities in both cases.

We also discussed the evaluation of the counterfeit threat scenarios using micro dynamic simulation. This modeling technique provides information needed for the quantification of economic risk exposure in conjunction with other analytical tools. It also allows the evaluation of the effectiveness of various on-chip risk management capabilities. And by generating test data, it allows the assessment of the effectiveness of the host system based counterfeit transaction detection models.

References

1. Ezawa, K.J. and Schuermann, T., "Fraud/Uncollectible Debt Detection Using a Bayesian Network Based Learning System: A Rare Binary Outcome with Mixed Data Structures," *Proeedings of the 11th Conference Uncertainty in Artificial Intelligence*, Morgan Kaufmann, pp. 157-166 (1995).
2. Ezawa, K.J., Singh, M., and Norton, S.W., "Learning Goal Oriented Bayesian Networks for Telecommunications Risk Management", *Proceedings of the 13th International Conference on Machine Learning*, Morgan Kaufmann (1996).
3. Ezawa, K.J., and Norton S., "Constructing Bayesian Networks to Predict Uncollectible Telecommunications Accounts," *IEEE EXPERT*, Vol. 11, No. 5, pp. 45-51 (1996).
4. Maher, D.P., "Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective," *Financial Cryptography '97 – First International Conference*, Springer Verlag (1997).
4. Porter, M.E., "Competitive Advantage," Free Press (1985).
5. Harding, A.(editor), "Microsimulation and Public Policy", North-Holland (1996).
6. Napiorkowski, G. and Borghard, W., "Modeling of Customer Response to Marketing of Local Telephone Services" in Dynamic Competitive Analysis in Marketing, Springer Verlag (1996).

Appendix



Originator Name : US

Segment Name bank1 □ Counterfiet

Average No. of Transactions:

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Lamda	2.00	1.00	2.00	1.00	2.00	3.00	4.00
Mean*	0.05	0.05	0.05	0.05	0.05	0.05	0.05
S.D. *	0.02	0.02	0.02	0.02	0.02	0.02	0.02

* : fraction of member having at least one transaction.

Minimum withdrawal 0.05

□ Load Consumers

Over night retention 0.05

Load hour 8

Member tx. amount 0.05

Deposit thresh-hold 0.1

Empty hour 16

Comments

Segment Type

○ Merchant Only

○ Consumer Only

● Consumer & Merchant

Figure 5. Example Input Screen - Member Segment Specification

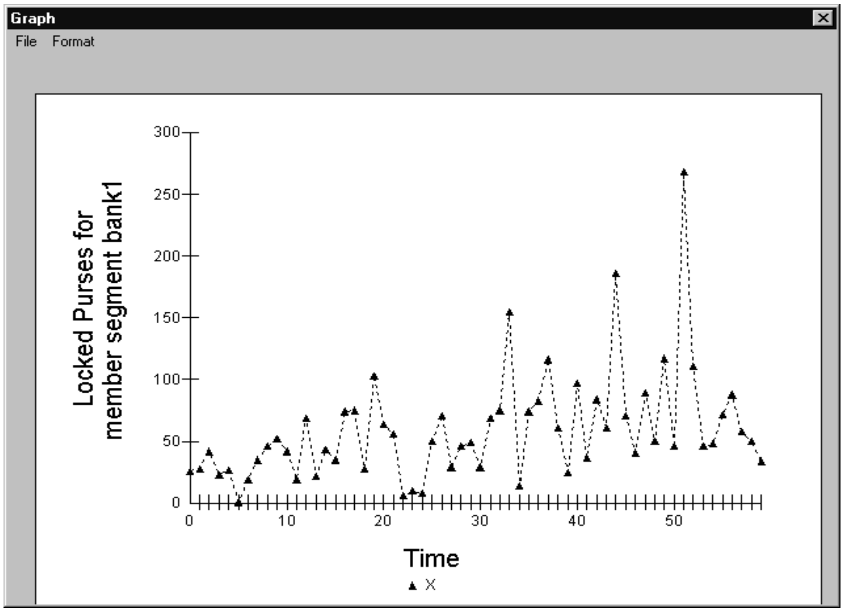


Figure 6. Example Output - Impact of Counterfeit Activity