Credit Card Issuer Fraud Management

Report Highlights

December, 2008

Principal Analyst

Ken Paterson

(781)-419-1715

kpaterson@mercatoradvisorygroup.com

TABLE OF CONTENTS

Introduction……..……3

I. Market Dynamics

And Now Back To Our Issuer Fraud Story……...…….……....4

Not My Loss—But Everyone Suffers…….……...…...……...5

II. SAS Fraud Management..……10

III. Shaping The Fraud Management Marketplace……..…12

The Enterprise Vision………….……12

Cardholders Are People Too (And They Vote With Their Feet)……..…..……12

TABLE OF FIGURES

Figure 1: Bank Card Issuer Fraud Loss Expenses Still Remain In A 40BP Cost Range …….....4

Figure 2: Fraud Losses Remain A Minor Direct Contributor To Card Issuer Expense ……..…5

Figure 3: Bank Card Fraud Expenses Rise With Volume ……..……..6

Figure 4: Total Credit Card-Related Fraud Losses: Probably $16B And Counting ……..7

Figure 5: Data Breaches: Intentional And Looking For Cards……..……..8

Figure 6: Mass Card Data Thefts Drive A Thriving Secondary Market In Card Products ……. 9

Figure 7: SAS Fraud Management: Bridging The Silos……10

Introduction

Report Highlights:

- 1. Credit card issuer losses remain surprisingly well-contained despite the continuing evolution of card fraud.
- 2. On the other hand, total fraud costs in the U.S. broadly related to credit cards alone is conservatively estimated to exceed $16 billion annually.
- 3. Purposeful data breaches are providing particular challenges to the industry, as criminals target easily-monetized payment card information.
- 4. The enterprise fraud management vision may have significant value, but organizational barriers remain high as issuers seek added detection lift from multi-product implementations.

As we discussed in our 2006 report on the issuer fraud solution topic, technology providers are increasingly focused on the vision of enterprise-level fraud solutions, and more broadly on enterprise financial crimes and risk management. Solution provider interest and capabilities are certainly growing in this regard. The enterprise vision could in theory address the "balloon effect" of fraud head-on, that is, watching for the inevitable shift in criminal activity from one product or business line to another under pressure from improved detection.

And why not stick with the siloed approach? Our overview shows that from an issuer's viewpoint, bank credit card fraud losses remain surprisingly well-contained at around $1 billion in the U.S., thanks to the effective solutions and services on the market. Unfortunately, cardholders might not agree. Both the headlines and market studies show that data breaches in particular are driving a thriving market in stolen card data. Secret Service/ Visa data actually put a market price on different combinations of stolen data. And then there is the vast array of other card-related and other account-based frauds. We take a SWAG that the direct costs of fraud attributable in some way to US credit cards could easily exceed $16 billion, without even taking in to account the financial institution's solution, staffing, and management costs.

No wonder major issuers are now advertising the fraud-fighting capabilities of their card services to potential cardholders—it is a high visibility issue, and banks have invested a lot. But it is a dynamic battle that extends well beyond the credit card product, and is nothing short of a battle to retain the consumer's trust.

I. Market Dynamics

And Now Back To Our Issuer Fraud Story…

When we last looked at card fraud losses, it was a relatively minor expense line for issuers. And the good news is that it still is. At about 1.2% of issuer expenses, and constrained to a narrow expense range over this decade, bank card fraud losses can be seen as a relative success story. In fact, after peaking over 18 basis points of volume in the early '90s, general purpose credit card losses have been at 7 basis points or lower during the present decade. Of course, a lot of work has gone in to engineering this stable performance, but more on that later.

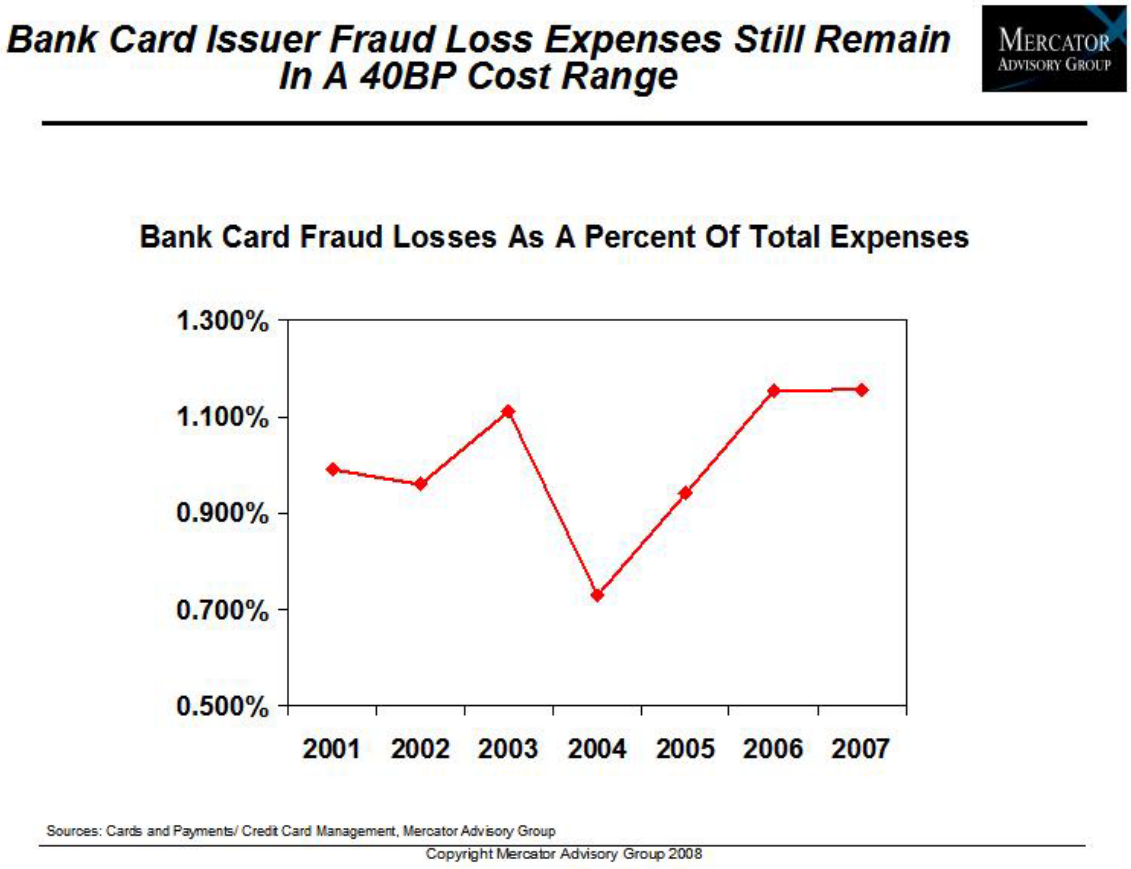

Figure 1: Bank Card Issuer Fraud Loss Expenses Still Remain In A 40BP Cost Range

Comparatively, fraud losses dwarf in comparison with the big three cost categories of operations, cost of funds, and charge-offs (see Figure 2). But to anticipate our discussion of hidden costs,

there are certainly hidden fraud costs in these numbers. Most notably in the $34.8B Operations and Marketing line item, there is surely a minimum of $2 billion in fraud solutions expense, IT, staffing, outsourcing, and outside data/investigation expenses embedded in this total. Plus, there is a literally unknowable component of Charge-offs that are misclassified fraud losses.

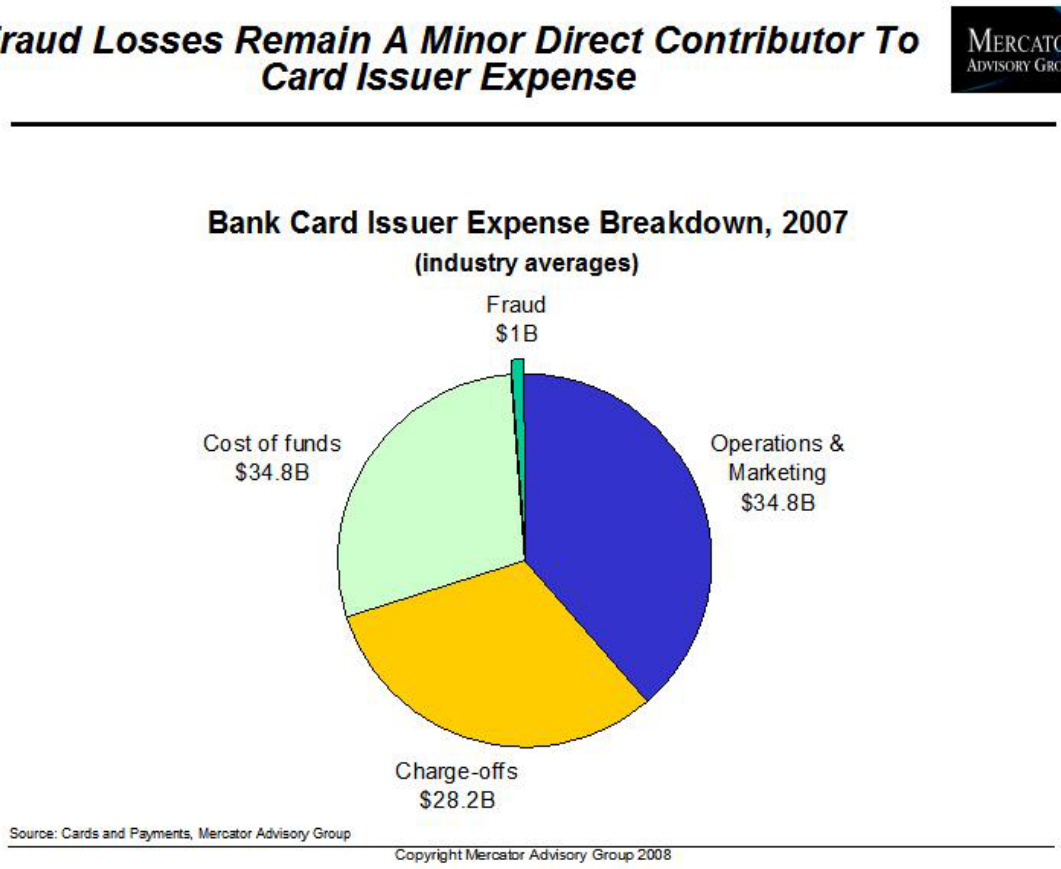

Figure 2: Fraud Losses Remain A Minor Direct Contributor To Card Issuer Expense

Plus, as an industry, total fraud losses escalate with growing payment volume. As Figure 3 illustrates, bank card fraud losses are up 55% since 2000, essentially parallel with card volume growth. But considering the escalating fraud challenges in the marketplace, these results have to be considered a glass half-full from the issuer viewpoint.

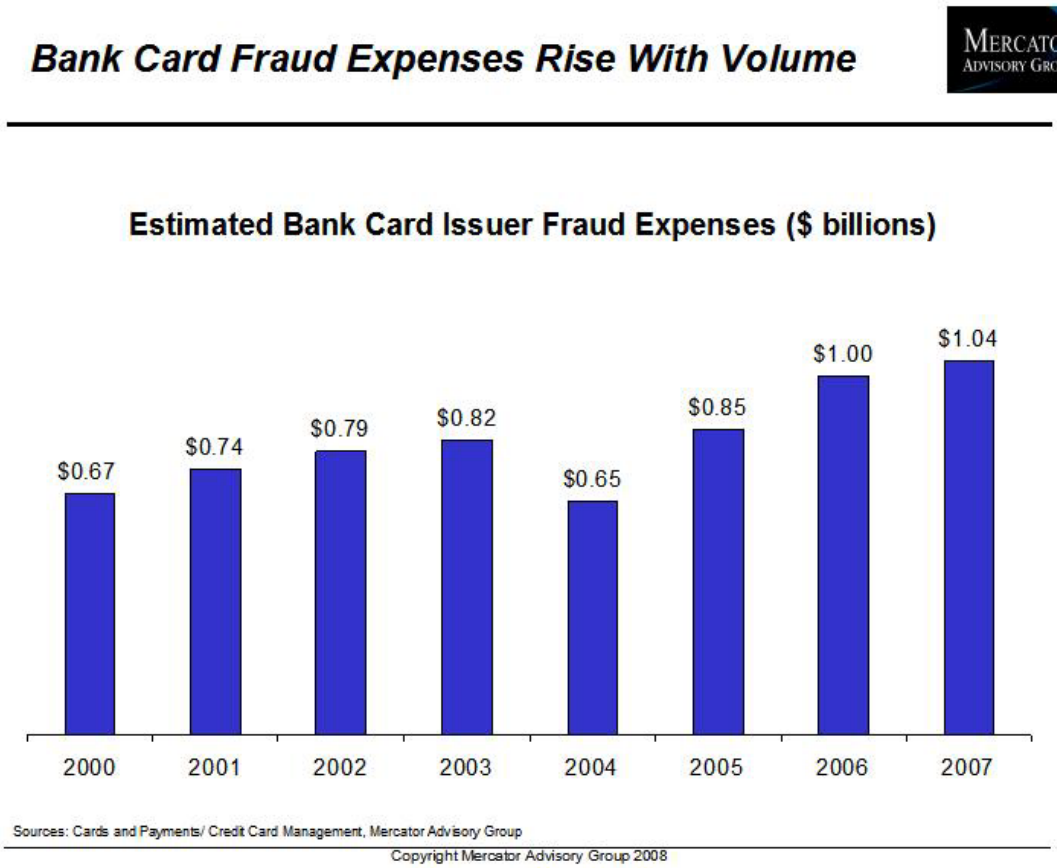

Figure 3: Bank Card Fraud Expenses Rise With Volume

Not My Loss—But Everyone Suffers

Taking the credit card issuer's viewpoint for losses understates the magnitude of the problem, and understates the risk to all the stakeholders associated with credit cards. The stakeholders tend to see different parts of the fraud elephant, some experiencing actual losses, while others experience virtual losses such as lost consumer spend. Figure 4 makes a stab at some of the major categories. Issuer losses (in this case all general purpose credit cards) come in close to the familiar $1B number and represent primarily card-present fraud, with online merchants absorbing perhaps twice that amount in card-not-present losses attributable to credit cards. Lost card usage--attributable to declined legitimate transactions, consumer substitution of other alternative payment types perceived to be safer, lost volume due to card cancellation and reissue—is an

opportunity cost certainly borne by credit card issuers and perhaps by some merchants. And lost usage is linked to potentially tarnished consumer perceptions of credit cards and/or their issuers. Consumer frauds peripheral to credit cards such as unneeded credit card insurance, advance-fee loan scams, and illegal credit repair could contribute to over $7B in direct expenses to consumers, not to speak of indirect costs, mental anguish, and potentially more damage to the reputation of credit cards.

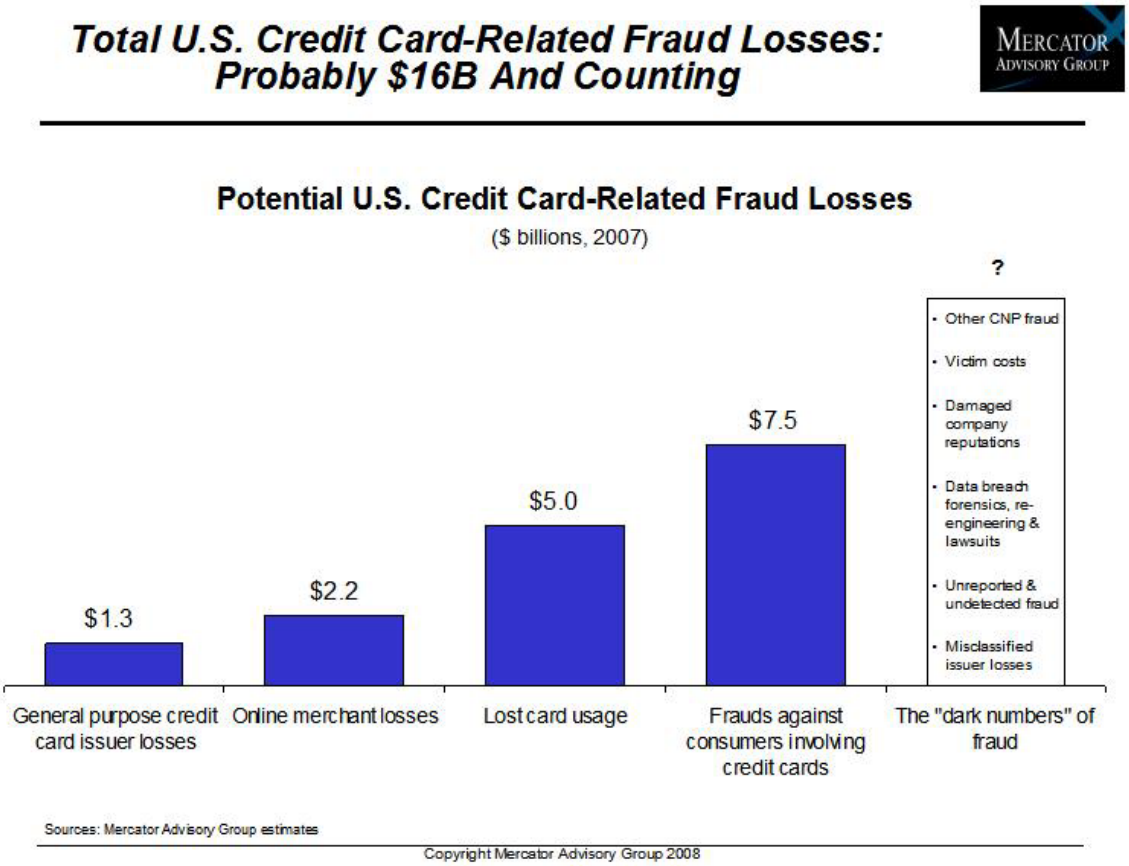

Figure 4: Total Credit Card-Related Fraud Losses: Probably $16B And Counting

In total, the unknown and unknowable costs (the "dark numbers" of fraud) are surely the largest, even after aggregating these estimated $16 billion in costs. In all likelihood, costs related to data breaches are significant in their own right, both in terms of remedial and legal expenses to the breached company, and in terms of the damaged reputations of these firms.

In fact, a recent Verizon study of over 500 data breaches reported between 2004 and 2007 is staggering in its implications. Of first concern is the deliberate and technologically sophisticated nature of the most frequent attacks. While some breaches are in fact opportunistic (abetted by lost or stolen laptops, thumb drives, paper copies, etc.), hacking and malicious code are the most frequent contributing causes. Second, the most frequent target of these attacks is in fact payment card data, often the most immediately monetized type of stolen data targets. While there is value to be had by criminals in broader identity information types such as those shown in Figure 5, card information has immediate market value and usability.

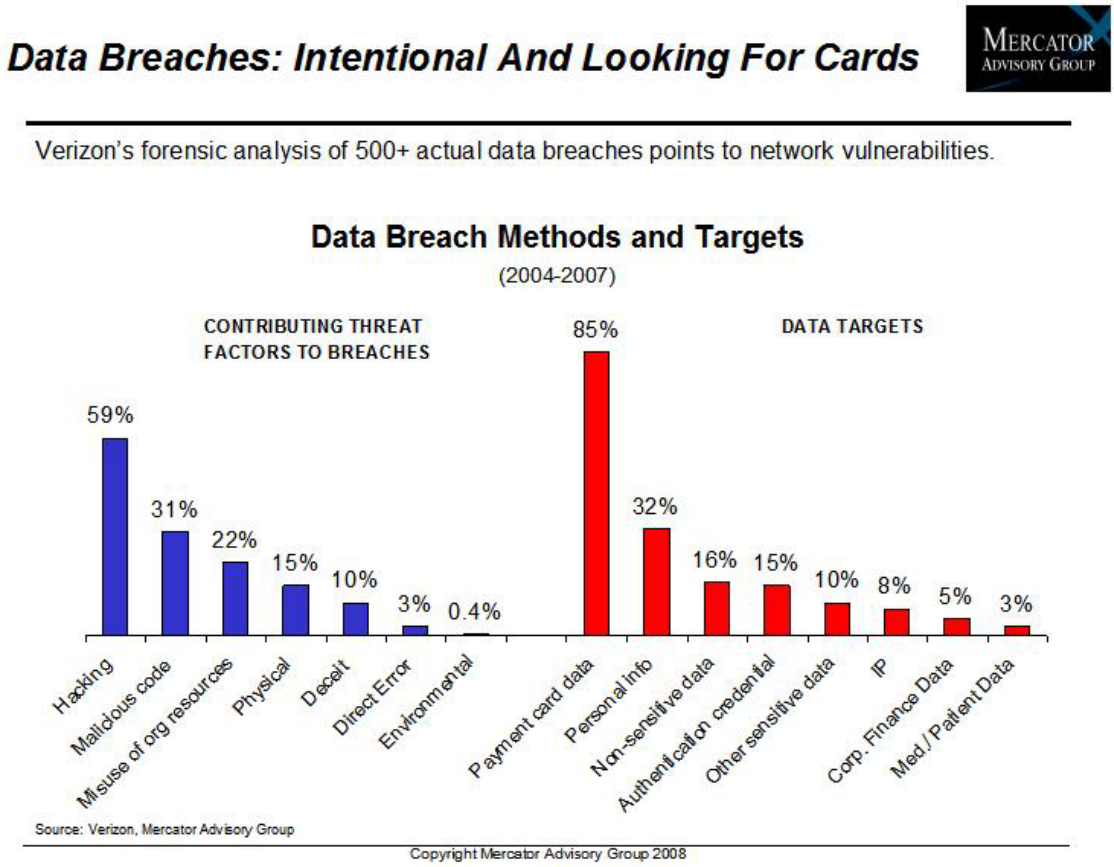

Figure 5: Data Breaches: Intentional And Looking For Cards

And speaking of the ability to monetize stolen card data, Visa and the Secret Service have recently published estimates of the market value of stolen card data. Value increases with the availability of track and PIN data, reaching its peak with a fully functioning counterfeit plastic.

The value of card data is apparent, and the motivation to pursue intentional breaches is certainly powerful.

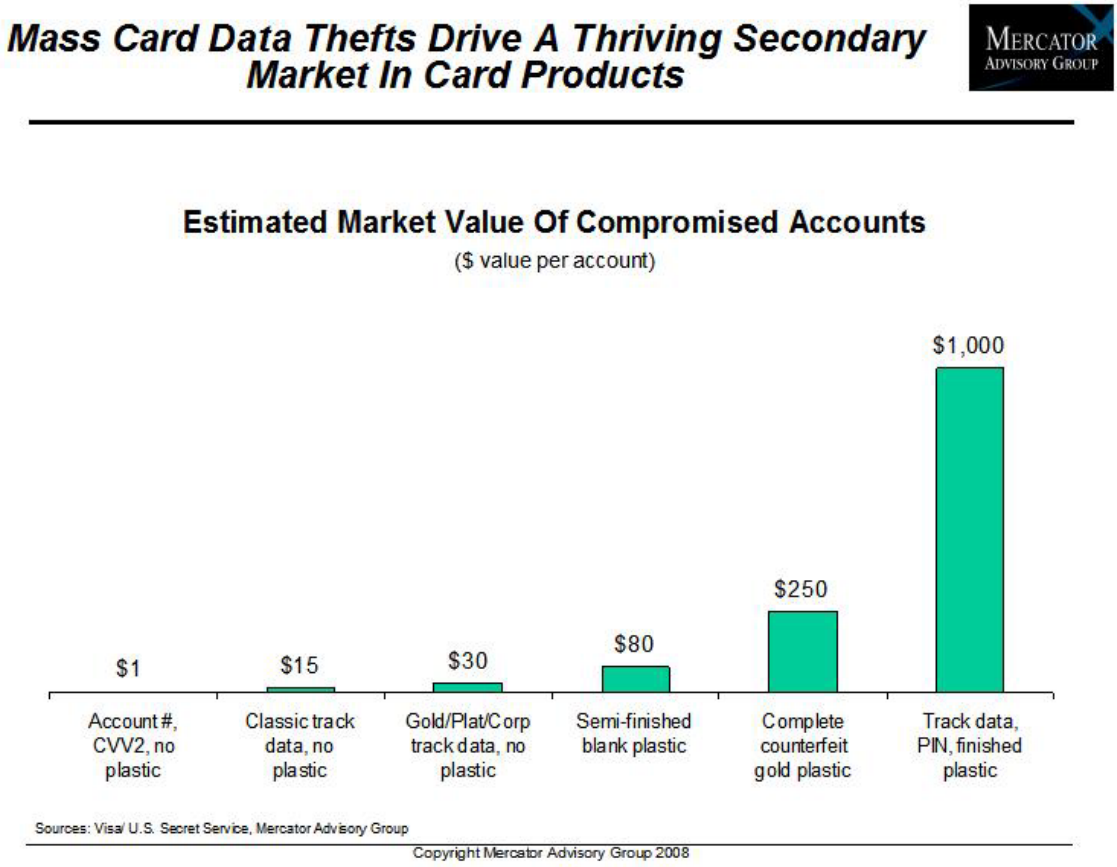

Figure 6: Mass Card Data Thefts Drive A Thriving Secondary Market In Card Products

Beyond these grim pictures is the reality that similar frauds affect debit cards and other payment products, as well as bank deposit and loan products. As the mere inconvenience of a stolen card number morphs into the more threatening label (and sometimes reality) of identity theft in the public's mind, no part of the FI is immune from financial or reputation risk.

II. SAS Fraud Management

SAS, the well known business intelligence software provider with some 3,000 FI clients, made headlines in the fraud management world with its announced signing of HSBC in 2005 with delivery in 2007 for its SAS® Fraud Management solution. Driven in part by its acquisition of Household International and its corresponding large card presence in the U.S., HSBC was seeking enterprise fraud detection capability that could be deployed globally, and within secured administration tiers. And, the goal was to detect fraud early, within 1-2 hits. HSBC represents a key client to illustrate SAS' enterprise focus and strengths, leveraging their Universal SAS Connector technology to access and link multiple account systems, making real the potential to detect fraud based on data across multiple product types.

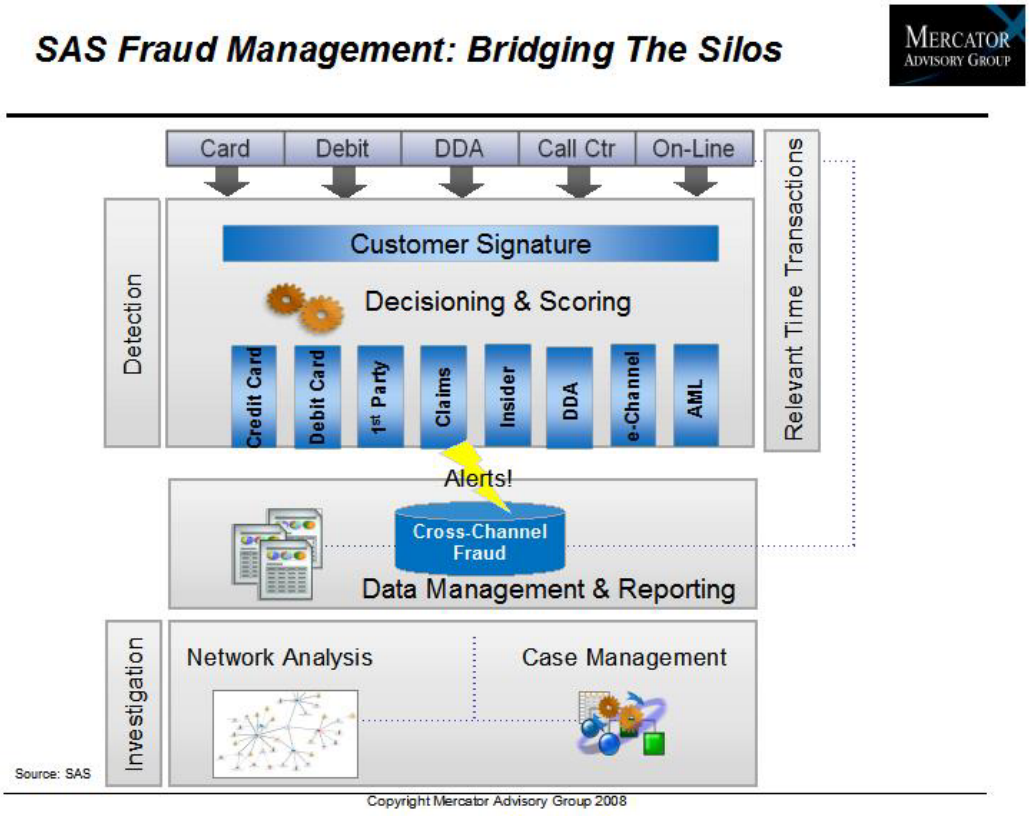

Figure 7: SAS Fraud Management: Bridging The Silos

In terms of real-time fraud scoring, the solution uses a combination of neural net and rules-based technologies, incorporating both consortium and issuer-customized models. Efficiency and scalability of the scoring solution are positioned as key sales points, with the claim that 100% of transactions can be scored during in-stream process, or "real time," and typically with less commitment of system resources. HSBC has published that they have seen a 12% decrease in mainframe processing overhead, while at the same time increasing their processing volumes by 87%. HSBC is said to be running several hundred rules in its implementation to complement the analytic models. Volumes of several hundred transactions/second are common. The ability to deploy and manage multiple fraud models across products and markets is featured, as well as the ability to conduct champion/challenger tests against competing models.

In addition to a case management module designed for managing suspicious accounts and triage-based alerts across multiple business lines, SAS has a unique Network Investigation & Analysis tool to support the users' ability to reveal and analyze network connections among all a cardholder's accounts and relationships. The main benefit is to help analysts visualize cardholder connections via network maps across product lines, although it can also generate customer risk scores—particularly useful in assessing account applications in real time. SAS notes particular success for this capability in identifying "bust-out" fraud and fraud mis-classified as credit losses—a real window into some of the "dark numbers" of credit card fraud we discussed in Section I.

III. Shaping The Fraud Management Marketplace

One of the problems in writing a report on the topic of fraud solutions is that we are not interviewing criminals regarding their development plans. So our viewpoint is by definition one-sided and reactive. But from our side of the fence, here are issues that will shape the credit card fraud management space:

- **The enterprise vision**

As mentioned earlier, the vision of enterprise fraud and/or financial crimes management is logical and appealing. It may in fact be more powerful in its fraud reduction capabilities within credit cards when additional product relationships are considered. We are definitely in the early days of enterprise fraud detection, where for some banks, "enterprise" may mean just the credit and debit product lines. Given the product similarities and their common processors, this should not be surprising. Data on the incremental detection lift of enterprise implementations—even if only for two product lines versus one—will be key motivators for firms considering this approach. But the potential value extends beyond fraud detection; the benefits to cardholders and retaining their business could be material.

- **Cardholders are people too (and they vote with their feet)**

As we commented earlier, it is all too easy to get caught up in the realities of risk management and keeping the losses of all stakeholders in check, and to ignore the viewpoint of the cardholder. The ultimate risk is: if cardholders are too concerned about fraud, or too confused about how it might impact them personally, they will switch cards, go back to cash, alternative payment systems when they are available, or switch entire retail banking relationships. As with all financial businesses, customer trust is at the heart of the business, and mixed, confusing, or threatening messages with regard to fraud could certainly affect that trust. The following issues will strongly affect consumer actions:

> **Fraud management as a marketing tool:** Issuers are already marketing their fraud management capabilities, including recent TV advertising from major issuers. It will be interesting to see if issuers begin to tout specific fraud detection capabilities, policies, or service guarantees. There is a fine line to tread between scary and reassuring, and consumer testing of features and advertising will be a critical developmental stage.

But for many consumers, the bottom line will be their experience when they call in to report an unauthorized charge or other suspicious activity. Just like auto insurers who get a bad reputation when they fumble claims servicing, issuers risk losing both a fraudulent transaction and a customer if the cardholder experience is not top-notch. The distance from top-of-wallet to back-of-wallet is not very far. And negative effects may jump from the wallet to the bank account as well, if consumers are angered both by the occurrence of fraud as well as how it is handled by their bank.

An issuer able to establish brand equity in consumer fraud protection could have a real advantage—reinforced every time a consumer reads a new report on identity theft or mass data breaches.

The double-edged sword of alerts: we commented earlier that with the escalating alert capabilities of issuers, alerts could easily move from a valued featured to a liability if consumers are overwhelmed. Cardholder control can provide part of the solution, with the user empowered to throttle the volume of information that is appropriate to his or her level of tolerance. But with multiple credit and debit cards in the wallet, each with varying control capabilities and alert policies, alert volume to any one consumer could become significant. The danger is that this new capability ultimately encourages consumers to turn off alerts, ignore alerts, or induces an unnecessarily high level of cardholder paranoia to the detriment of card usage.

Ultimately, industry consensus must emerge around the right types of alerts to push out, and standard consumer interfaces to control them. And of course, if the detection technologies are highlighting real fraudulent transactions (not false positives), issuers will be simultaneously minimizing consumer awareness of their false positives. In the immediate future, issuers will have the added complexity of managing both their fraud detection parameters and their communication parameters for cardholders. And driving alerts to consumers also means the potential for higher call center volumes and the need to carefully manage the handling of these calls.