Jennifer J Johnson
Secretary, Board of Governors of the Federal Reserve System
20th St. and Constitution Ave. NW
Washington, DC 20551

Re: **FRAUD COST AND INTERCHANGE**

by George Cox
February 21, 2011

Dear Ms. Johnson:

Thank you for the opportunity to comment on the Federal Reserve Board's proposed changes to interchange rules. My comments speak to **Section 235.4 Adjustment for fraud-prevention costs.**

Fraud cost captured in the current framework of interchange has failed to improve social benefits to debit card holders and has only served to maximize card issuer, acquirer, and card association revenue. Two factor authentications of PIN and Signature on different networks has also failed to prevent fraud or protect card holders. Fraud cost must necessarily be captured in interchange fee. Fraud costs encapsulated in interchange must be decoupled from merchant or industry credit risk score and be tied back to segmentation by fraud products that advance technological security processes on behalf of cardholder's their account numbers are breached. In other words fraud costs must be bifurcated from credit risk cost in interchange. Furthermore, the highest form of security must be in a card independent security feature. This answers question #1 of the DRAFT as this is a different approach to establishing the adjustment standards that the Board is considering. Unlike the card dependent magnetic stripe, expiration date, PIN, Signature, smart chip, or other inherently flawed product. This is best achieved in advancing biometric technologies during all card transactions. I close with a stair step or incremental costing framework for capturing fraud costs.

CURRENT INTERCHANGE AND FRAUD

Debit card fraud, which includes POS, PIN, and ATM transactions are directly linked to checking and savings accounts and can wipe out consumer's life savings instantly. Ninety-two percent (92%) of Community and mid-sized banks and ALL the large institutions ($10B>) reported having losses from debit card fraud in 2008. Debit card fraud now causes financial loss to a higher number of banks than check fraud does. *(Source: ABA Deposit Account Fraud Survey 2009).* Thieves have made these accounts a priority because of the direct link to cash. Fraud represents a serious threat to the stability of our Nation's credit markets. Interchange in its current state fails to advance technological improvements to prevent fraud that may lead to social benefits for consumers. In fact, interchange in its current state reinforces profit maximization and falls far short of Ramsey pricing. Why? Interchange in its current state merely considers merchant history of fraud, industry history of fraud, geographical location of the card acceptance, chargeback history of the merchant, size of the merchant, dispute history of the merchant, and other credit risk factors (emphasis supplied). These variables have set the interchange fee in the United States and have failed to segment fraud prevention processes. Fraud costs are wrapped into credit risk and thus distort the picture of both. So for example an industry that provides goods or services after you buy it (airlines or CPS/Passenger Transport) has a higher interchange fee e.g. (1.75%+0.10) in relation to an industry that provides goods or services before consumption (grocer or CPS/Supermarket –Performance Threshold I (35 million+ transactions) has a lower interchange fee e.g. (1.15% +0.05). The current rationale is that consumers might switch or cancel airline tickets before consumption thereby triggering chargebacks which push retailers in a higher credit risk category. This requires representment and man-hour cost to acquirers to remove the credit from the merchant's bank account. However, many of these

industries have outpaced these high interchange fees by discouraging such transactions with cancelation fees, restocking fees, switching fees and similar. The current interchange climate fails to segment fraud prevention products available in the market place and treats them all homogenous with no social benefit to the consumer. The costs and benefits are not the same.

FRAUD PRODUCT SEGMENTATION and INTERCHANGE

The leading debit card fraud categories include counterfeit cards for signature debit or white plastic (37% of 2008 loses); and stolen cards for PIN debit (45% of POS PIN debit loses; and 42% of ATM PIN debit loses) *(Source: ABA Deposit Account Fraud Survey 2009).* This is inapposite to the Federal Reserve's subjective survey which indicated Signature was higher than PIN perhaps due to volume (see footnote 67). Regardless, the two factor authentication of PIN and magnetic stripe or Signature and magnetic stripe has not prevented fraud. This answers question #2 of the DRAFT as to the likely effectiveness and cost effectiveness of these fraud products. Further to that point interchange in its current state fails to advance fraud prevention.

Interchange has consistently failed to incentivize segmented fraud products. It has instead lumped all security approaches together wrapped inside credit risk. The security features embedded in the card are inherently flawed and interchange for fraud is treated homogenously and not segmented by security product. Greater emphasis should be applied to security apart from the card and less weight given to security embedded on the card. Before a security guard can protect the building, the security guard must first be protected in a booth, command center, or similar- otherwise they run the risk of their safety being compromised. This is sometimes referred to as the Chinese wall.

The same concept goes with cards. For if the above PIN, Signature, or chip-n-PIN, pictures on cards, mobile payments, or similar card dependent security features fall into the criminals' hands, why then it is merely a small matter of reverse engineering to garner the gold nuggets for account hijacking *(see NY Times dated June 10, 1998)*.

The semi-conductor chip found on the Smart Card uses electrons to perform algorithms, and the flow of electrons were measured with a simple attachment to a personal computer. The measurements of the flow of electrons when neutralized render the chip on the card worthless. Each card dependent security product like PIN, password, or similar raises the problem of verifying that the presenter is the authorized user and not an unauthorized holder. PCI/DSS standards are helpful but merely reduce the amount of data in storage. The amount of data in motion remains a threat vector even in end-to-end encryption. This is due to man-in-the-middle attacks and packet injections. Interchange fails to incentivize card independent fraud prevention.

In fact if a victim's card number falls into the hands of a card thief, then typically with a little reverse engineering of the magnetic stripe data along with a bit of social engineering, the savvy criminal may easily open new accounts in the victim's name. This is because the underlying cardholder's information stored on the card is card dependent. Thereafter, the newly assigned PIN and Signature, or end-to-end encryption, or newly issued tokenization, or dynamic data of the newly opened account merely reinforces the fraud. Thereafter, card issuer's revenue increases and write-offs ensue to society. This current framework has staved off investment in security. So, despite the legitimate card, the new account is still fraudulent and consumers absorb the expense in the form of higher interchange, reputational loss, years of name repairment with no social benefits. This holds true because the merchant's credit risk factors and chargebacks

either increase in the case of a dispute or fine imposed at the end of the victim's billing cycle. Further to that point, if the fraudulent card is used at the airline or grocers with either PIN or Signature as mentioned above, interchange merely evaluates the type of transaction (pre or post consumption), industry history, merchant history as relates to their credit risk and fails to advance technological social improvements for card holder protection. Interchange is silent on segmentation of the security product.

Card independent security must be given greater weight to justify higher interchange than under the current card dependent security flaws. So for example PIN, Signature, and Smart Cards should have a lower interchange due to its decreased social benefit to consumers. Whereas biometrics, holograms, liveness detection, and even call-back (landlines not mobile phones that get lost/stolen) with passwords along with other card independent security features that are not stored on the card should necessarily have a higher interchange due to its increased social benefit to consumers and cost to card issuers. Fraud products should be segmented with standards that advance technological improvements for enhanced social benefits to the consumer.

I therefore am in favor of a non-prescriptive approach because (1) the technology specific industry representatives failed to include biometrics; (2) The technology specific approach would cause issuers to under-invest in new emerging technologies which is counter-intuitive to social benefits advanced in this white paper in an effort to stay ahead of the bad guys; (3) The non-prescriptive approach would be set for the issuer to recover some or all of the costs of emerging technologies as hackers get more savvy; (4) Non-prescriptive approach would allow issuers to recover some or all of their research and development for new fraud-prevention techniques, perhaps up to cap (which I am opposed too, yet argue should be indexed if imposed); (5) As

stated, the other approach to establishing the adjustment for standards that the Board should consider should necessarily be grounded in product segmentation as measured by the social benefit to the consumer and incentive for technological advances to prevent fraud in the first place with greater weight afforded to card independent security approaches. Fraud prevention is a function of dynamic countermeasures not a function of static threat vectors e.g. PIN or signature.

ROUTING

It is apparent that merchant's ability to use different networks (PIN v Signature) or one network to reduce their pass thru fees has not prevented fraud. This has been proven in Australia where the savings enjoyed by merchants who chose a cheaper network were not passed along to consumers. Debit card routing for POS PIN, ATM, or Signature in a multi-home network fails to prevent fraud but merely maximizes profit for the merchant and acquirer. It has also allowed issuers to evade interchange ceiling limits by receiving net compensation from network access fees without considering the cost of fraud segmentation products along the network. Once again the card holder pays the same price for goods/services despite the network used.

This writer would be in favor of issuer's capturing network processing fees resulting in higher interchange if it resulted in justifiably improved social benefits in the form of product segmentation for enhanced security. I would be in opposition to caps at the issuer or network level because they would fail to capture full fraud costs. Again, greater weight should be afforded card independent security features. Routing in its current state is silent on this issue. Today's network message routing is not dedicated to debit cards but is also used for utility bill payment, and card top up (mobile phones and prepaid cards), local events and advertising.

This underscores why security must be segmented by product and not by network or issuer as relates to interchange cost structures for security.

It is also noteworthy that interchange should be indifferent as to how a transaction is facilitated. If a card holders uses a swipe machine, card insertion device, tap-n-go, contactless RFID, mobile payments, third party digital cash, third party network, Pulse, NYCE, Interlink, STAR systems, private network or Visa/MasterCard; the element of fraud still exists and one may argue is elevated due to the emphasis on speed and convenience with the continued dependency of security on the card. E.g. CVV numbers are embedded on the mag stripe along with expiration date, card issuer bank identification number (BIN), card account number, and other card dependency security features tightly coupled with the card or mobile phone. All of the fields on the magnetic stripe tracks were introduced to facilitate the transaction and reconciliation process only and were never intend to prevent fraud. Interchange can now play a role to enhance security.

REASONABLE AND PROPORTIONAL

NO-CAP ON INTERCHANGE MUST INCENTIVIZE QUALITY OF FRAUD PREVENTION

Interchange fraud standards must be tied to the segmented security tool cost to prevent fraud in the first place thereby justifying a higher interchange fee. This will improve social welfare. Standards for fraud must necessarily be bifurcated away from credit risk of merchant history, size, type of transaction, brand card, network, industry, geography and other meaningless variables that fail to protect the consumer that have traditionally emphasized credit risk and profit maximization. Standards must be adjusted separately for recoupment of fraud product segmentation.

One solution advanced in this paper might be technological advances for card independent biometric facial recognition. There may be other card independent security tools available such as holograms, liveness detection, and others. These may be considered a social benefit of fraud prevention and thereby garner a justifiably higher interchange.

Conversely, Signature, PIN or other card dependent security features might be considered a lower layer of security and merely maximizes profits at the expense of social welfare and thereby garner a justifiably lower interchange or ceiling.

CAP ON INTERCHANGE MUST INCENTIVIZE QUALITY OF FRAUD PREVENTION

On the other hand should a cap (the proposed $0.12 cents) be imposed on the existing framework of merchant credit risk then a larger portion of interchange must be allocated to card issuers for card independent security tools like biometric security because issuers' fraud risk is reduced and their cost structure has increased. For example, on a $100 transaction, $0.01 cents must go to the merchant discount fee and $0.11 cents to the card issuer. Although a twelve cents cap and seven cents safe harbor will be at the detriment of investing in improved security.

Conversely and under the existing and old merchant credit risk framework with the use of card dependent security tool Signature or PIN why then a smaller portion of interchange must be allocated to card issuers. For example, on a $100 transaction, $0.11 cents must go to the merchant discount fee and $0.01 cents to the card issuer. This is because the merchant and consumer now bear the highest risk of fraud, disputes, chargebacks, lost of goods/services, reputational harm with the use of these low level card dependent security tools.

Card issuers merely make up the difference in revenue from raising annual fees, over-the-limit, late fees, and other fees with no concentration on fraud prevention segmentation standards and consumers continue to be disproportionally burdened.

HOW SHOULD NON PRESCRIPTIVE STANDARDS BE SET?

An index should be established and stacked against each existing segmented security product to stair-step or increment to recover cost in a framework pursuant to the security models advanced in this white paper. The cost based interchange must necessarily be tied to the cost to the card issuer or card associations to acquire, produce, deploy, license, contract, study, test, research, develop and maintain the card independent security tools. As regards to question #7 in the DRAFT, Biometric standards and cost structures may be obtained from The U.S. National Biometric Test Center, The National Institute of Science and Technology (NIST), as well as the Center for Biometric Study at the University of West Virginia who has been receiving Congressional discretionary funding for years for these very purposes. Distortions in the economy will results in job growth in multiple areas from engineering to call center activities and peripheral green offshoots.

A sample stair-step or incremental cost recovery standard for fraud might be: Smart Cards cost five dollars and up and run about five to ten times the cost of a magnetic stripe card. This depends on the amount of silicon wafer and the configuration of the Smart Card and merchant upgrade. Thus working backwards, facial biometric would garner a higher cost recoupment than fingerprint recognition systems according to Frost and Sullivan industry analyst Sapna Capoor. And smart cards would garner a higher cost recoupment than PIN and PIN would garner a higher recoupment than Signature based on the cost structure for implementation. This would result in a

proportionality identical cost-to-fee ratio for all covered issuers and remove issuer specific cost variables e.g. geographical location, staffing expertise, MSA fraud susceptibility, local or regional crime rates.

I am opposed to a cap, yet if one were imposed on all or some cost, then social benefits of job creation and other variables could offset the cap limitations. Social benefits will be measured by the product's elimination of fraud, where one fraudulent activity is too much and that product drops down into a lower category. Essentially the measurement should be against each other security product's effectiveness to prevent fraud. Then you have a race to the top.

The Board can effectively measure fraud prevention by the number of imposters that are declined by the merchant at the POS. Data security costs for the 8 million merchants in the U.S. under my product is less than 0.2 cents p/transaction. I have developed a simple software download for the merchant's computer based point-of-sale terminal so they enjoy zero hardware upgrade expense, unlike smart cards, encryption overhead, or others. I have made facial biometrics cheap and effective to deploy and also measure effectiveness. See it in action here: www.headsup.cc

Working forward, and as regards to question #5 of the DRAFT, the idea on the fee methodology must be to create more value on the higher end by offsetting the fee difference. The goal is to say to the market, "By investing in Signature and passwords, you will receive the basic revenue stream with no social benefits and full responsibility for fraudulent transactions remains with the card issuer. However, for more investment you can enjoy Smart Cards or PIN which will provide a middle of the road revenue stream with some social benefits and full responsibility for fraudulent transactions remains with the card issuer. And for just a little more investment, you can enjoy Facial Biometrics which has all the benefits of Signature, passwords, PIN, and Smart

Cards plus full social benefits to the consumer and full responsibility for fraudulent transactions shifts to the merchant! Costs measurements and effectiveness for PIN, Signature, Smart Cards, end-to-end encryption, and tokenization are already in the marketplace.

Research shows that markets will lean toward the higher end if they perceive the difference in value to be greater than the difference in price. Further, it is critical to brand the high end and make it the benchmark. Under the non-prescriptive approach the benchmark may easily be adjusted as new technologies emerge in an effort to stay ahead of the bad guys. Events that could trigger review:

1. When the cost of capital rises to a pre-determined level this compels consumers to use cards more often thereby triggering a review. The best time to review fraud is not in a fraud crisis.

2. When truly new preventive products are introduced at conferences, the marketplace, through a call for papers, or other avenues. For example telephone call backs, credit monitoring freezes/thaws are all card independent security, yet they are reactionary. In that I mean the security takes place after victimization. Emphasis must applied to prevention beforehand as in the case of facial biometrics.

3. When the voluntary membership into a particular security product by consumers falls below a pre-determined level. This speaks to customer acceptance. Although this could be rendered moot if this rule is mandated in cardholder or merchant agreements. This goes back to effectiveness. Perhaps more study is required on review times and I am coming closer to the deadline for submission of this writing.

EQUILIBRIUM INDICATORS

Either approach reduces the Gini Coefficient of our Nation to the extent that fraud exerts a high price on our citizen's hard earned life savings, stable credit markets, victim's good name and credit histories, and the judicial expense in investigating and prosecuting criminals. Today many of the criminals operate outside the purview of the United States and may be found in Malysia, Nigeria, or China. This costs our Department of Justice and Bureau of Prisons and Law Enforcement investigative man-hours and limited resources. Already States like Virginia have passed HR 454 Title 19.2 Chapter 6.1 legislating Orders for Facial Recognition Technology. It is important to take steps to stay ahead of the bad guys. Judicial limited resources may be reallocated more efficiently once this plan is adopted.

SUMMARY

Reasonable and proportional interchange fraud expense must be segmented by security product and the social benefits conveyed to the consumer not just issuer and acquirer or merchant. Interchange in its current form merely lumps all security products into one when clearly the cost structure and social benefits are discreet. The objective should be to incentivize technological advancements in card independent security features along the product segmentation value chain with one example being biometrics for social benefits to consumers to prevent fraud. An incremental recovery cost structure indexed against other security products was suggested. Objective costs are either deployed or may be found at National agencies and State Universities. Measurements of effectiveness should also be indexed against each other where one is too many. That results in a race to the top to stay ahead of the bad guys and stabilize our markets.

George Cox is CEO of www.HeadsUp.cc, a cyber security start-up in Harlem USA that is currently in the fund-raising stage. The firm specializes in Point of Sale transaction security and facial biometrics during card transactions. An honorably discharged United States Air Force Veteran, he is also a network engineer and certified ethical hacker who earned an academic scholarship in banking and completed his degree requirements within three years at Saint Louis University. He also worked at the graduate level in computer science at North Carolina Agricultural and Technical State University. He may be reached for comments

Thank You Kindly,

George Cox