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

Re: Interim Fraud Adjustment Rule
Docket No. R - 1404
by George Cox for HeadsUp, LLC
Date: September 29th, 2011

Dear Ms. Johnson:

Thank you for the opportunity to comment on the Federal Reserve Board's proposed changes to the adjustment on the interim rule for fraud-prevention activities and costs.

HeadsUp is a consumer advocate and technology company specializing in facial biometric recognition for authentication at the point of interaction for card transactions including debit cards. As regards to authentication, clearance, and settlement this comment will focus exclusively on the authentication step. HeadsUp is in accord with the "Board's concern in that limiting an adjustment to authentication methods available today (Signature, PIN, Dynamic Data, Transaction Monitoring aka Neural Networks, PIN customization, Card activation, EMV chip, or Telephone call back), or a subset of those methods, may limit issuers in developing other methods of authentication that may be more effective than today's alternatives that may not require a PIN. It may also reduce the incentives for issuers to improve fraud-prevention techniques for systems that, for a variety of reasons, experience higher fraud rates." (See draft pg 362 – 363).

Under EFTA Section 920(a)(5), the Board may allow for an adjustment to an interchange transaction fee amount received or charged by an issuer if (1) such adjustment is reasonably necessary to make allowance for costs incurred by the issuer in preventing fraud in relation to

electronic debit card transactions involving that issuer, and (2) the issuer complies with fraud-prevention standards established by the Board.

This white paper advances Biometric Facial Recognition (BFR) authentication and respectfully asks that the Board invoke "such other factors as the Board considers appropriate" in reaching the "reasonably necessary" cost basis of fraud prevention activity costs for the 21st Century. The *requirement that issuers take effective steps to reduce the occurrence of, and costs from, fraud in relation to electronic debit transactions, including through the development and implementation of cost-effective fraud-prevention technology* must necessarily consider allowance for costs for Biometric Facial Recognition technology. This technology is available today yet is stifled to the issuer in preventing fraud because the current interchange climate has reduced incentives for active involvement of all five key players in a debit card transaction at preventing fraud. Instead it has merely incentivized merchant volume and not fraud-prevention. The result has been a hodgepodge of passive sporadic attempts at fraud prevention. (See Draft page 347)

THE INTERIM ONE CENTS ADJUSTMENT IS FLAWED

The Board reached the interim one cent adjustment found on page 49 in the draft as follows. *Issuer fraud-prevention and data-security costs*. The median issuer cost for all debit-card related fraud-prevention activities (excluding data security costs, which were reported separately) was approximately 1.7 cents and the 80th percentile was 3.1 cents. The most commonly reported fraud-prevention activity was transaction monitoring. The median issuer cost for transaction monitoring was 0.7 cents, and the 80th percentile was 1.2 cents. The remaining costs related to a variety of fraud-prevention activities, including research and development, card activation

systems, PIN customization, merchant blocking, and card authentication systems; the per-transaction cost of each individual activity was small, typically less than one-tenth of a cent each. The median total data-security cost reported by issuers was approximately 0.1 cents and the 80th percentile was 0.4 cents.

This retrogressive look at arriving at one cent fails to take into account the costs that issuers incur from adopting materially more effective and emerging forward looking fraud prevention tools such as facial biometric technologies for the 21st Century. Even the flawed EuroPay, MasterCard, Visa (EMV) chip technology available today yet easily exploited by Cambridge University students has costs to the issuer that has not been included in the Board's current interim adjustment. If issuers attempted to advance this flawed technology the interim rule would fail them as has biometric facial recognition and perhaps hologram authentication one day in the future. The final rule must necessarily incentivize adoption of BFR by issuers.

HOW OUR BIOMETRIC FACIAL RECOGNITION WORKS

Our patented pending system works once a debit card holder uploads his/her accepted facial image to our secure website. We then match the image and debit card holder against our gallery of images within our proprietary software. Multiple exhaustive tests are performed and our targets are achieved including but not limited to our floor and ceiling limits. We then are close to completion of our back end primary account holder pre-authentication process if our quality control and assurance Officers are satisfied with the results of the tests performed. On a cost/benefit analysis it becomes too expensive for a thief to impersonate a card holder by way of plastic surgery for just one account hijacking. Our proprietary software integrated into our facial biometric system requires and uses live-detection thermal imaging along with 3-Dimensional

capabilities. This prevents a prevaricator from being able to download a potential victim's *facebook* picture or a surreptitiously smart phone snap of a picture of a potential victim, for example, and then attempt to upload it to us as that potential victim. This would force a denial on the issuer's system. In the next step we store the image data points into our secure database. Finally, when the debit card holder uses their card either through a magnetic swipe device, card insertion device, manual input, near field communication (NFC), mobile phone, or other debit card transaction as defined, then our system will contact the issuer and upon approval our patented pending system will electronically transmit the card holder's facial image to the merchant's point of interaction all within six seconds. There is no added expense to the merchant to upgrade their hardware. Our authentication process starts with the issuer before the transaction is approved or denied. Therefore the issuer is expensed for the total cost of biometric facial recognition. Uniquely all five key players (issuers, card holder, acquirer, merchant, and card association) perform a proactive function in BFR at the authentication step. This results in a materially more effective fraud-prevention tool that immensely benefits all five key stakeholders along the value chain. This is forward looking and may have escaped the Board's purview during the interim rule.

THE FIVE KEY PLAYERS ACTIVE INVOLVEMENT

Involving the consumer in debit card fraud-prevention is a step issuers must take. BFR empowers the issuer to involve the consumer during active picture taking. The issuer also empowers the merchant to compare/contrast the pre-authenticated card holder with the person standing in front of them at the time of the card present transactions. This allows the merchant to be active and not passive. It allows the merchant to be involved first-hand and not be beholding

to each issuer's lack of a ubiquitous standard hodgepodge of fraud prevention tool such as an RSA token or EMV Chip which describes the interchange climate in its current state. BFR requires that the acquirer be actively involved. This holds true when the issuer is unavailable for approval or denial or when the issuer is offline. Here the acquirer necessarily absorbs the risk in the interim based on the issuer's predefined parameters associated with the BFR authentication. When the issuer comes back online, then the transactions may be batched, from a store-n-forward paradigm that the acquirer's system operates within. And finally card association play an active role in BFR in creating, adopting, implementing, and incentivizing transaction codes and or promotions to advance the technology. This writer is therefore in favor of issuer based promotions for BFR or for that matter, merchant based promotions as well. Whatever it takes to push pass the old flawed technologies.

Issuers are best poised to authenticate their card holders via BFR at the point of interaction based on consumer parameters. Acquirers and merchants enjoy reduced chargeback and representment expenses as well as fines imposed that may be attributed to fraud. Merchants also fear having their merchant accounts closed and may suffer from loss of goods sold, shipping cost, card association fees or fines, and acquirer fees. BFR actively involves merchants who have a great deal at stake. BFR also reduces issuer administrative expense on State required mail-out notifications, card production and delivery, new account or day one fraud, reputation damage, and a host of other related expenses. BFR stabilizes our credit markets in that the credit that a merchant expected on a cash or accrual basis from a debit card transaction is now no longer tied up in the 180 day dispute period due to fraud. In fact fraud dispute is eliminated with biometric facial recognition.

FACIAL BIOMETRIC COSTS

Our cost of research, developing, capturing, storing, pre- authenticating, and then very, very quickly and electronically transmitting BFR to a point of interaction on a per transaction basis is four cents (4.0 cents). Although fully absorbed by issuers, it is apparent that issuers may best be poised to spread their cost across all five key players in the debit card transaction and should be able to recoup the full amount. As we shall see, uniquely BFR actively involves all five key players in apposite to all other tools with the sole exception of merchant blocking. Our cost study was conducted on a volume of 200 million debit card transactions during peak and off peak performance hits to our main servers. Our effective success recognition rate is ninety-eight percent (98%) in our test market study with a sample size of 200 million images. We back this up by testing our technology at an Identical Twins Convention held in Minnesota where our results were consistent with our test market study, despite the likeness in similarities. We boast such a high success rate relative to low false positives and low cost primarily due to the active involvement of the card holder's voluntarily opt-in participation to sit for their picture to protect their good name and credit history consistent with our lighting and overall instructions. This may be contrasted against passive BFR for example at a sporting event, where the false positives are higher due to lighting, obtuse angles, and a host of other variable. It is apparent and practical for issuers to adopt BFR because all five players consisting of issuer, consumer, merchant, acquirer, and card association all benefit from BFR authentication process materially and more effectively than the current flawed methods sporadically used by different stakeholder at different phases with different platforms to prevent fraud. The absence of a standard actively involving all five key players has created a hot bed of threat vectors for would be thieves.

NATURE & TYPE OF TODAY'S SOPHISTICATED FRAUD

BFR necessarily shifts liability onto issuers in preventing cross-channel fraud schemes such as account takeover, mobile app and smartphone apps security flaws, mobile malware, ATM skimming, Insider Gary Foster or Tamara Moon Fraud, out-of-band authentication, RSA Secure-ID breach, and similar issuer fraud vulnerabilities. BFR technology also has future application potential during card-not-present transactions or mail order/telephone order (MOTO) as well as to prevent Automated Clearing House (ACH) and wire fraud during the settlement step. BFR may also be implemented for both retail and commercial accounts in addition to the consumer accounts as promulgated in this rule.

As of this writing the current interchange climate has impeded research, development, and implementation of BFR which is economically available today provided the interchange climate incentivizes such technology. A closer look at the current interchange climate reveals that with a small investment on the mechanical side; a small group of well funded and well organized crime syndicates perhaps based in Sri-Lanka, Malaysia, or Bulgaria may garner the international proliferation of contraband skimming devices easily found on the Web. Thus one can steal millions of dollars through skimming with counterfeit cards. It raises the question on why these devices are not regulated and more importantly why the card associations have not been pushing for such a thing. Smart cards (EMV chips) would not prevent this type of fraud because the security feature rests on the card itself which is inherently flawed. A Thief merely needs to capture the card's info and then with reverse engineering, simply duplicate it, then steal the golden nuggets. (*see NY Times June 22, 1998- Code Breakers crack smart cards' digital safe, by Peter Wayner).* This is a 21st Century war that has taken a cross-border reach and has spanned

into the United Kingdom, mainland Europe as well as here in North America. The current interchange climate merely incentivizes merchant transaction volume and not fraud-prevention. Moreover it haphazardly and sporadically incentivizes passive involvement of some of the five key players irregularly.

THE FRAUD ADJUSTMENT NEW PARADIGM SOLUTION

Authentication fraud-prevention must necessarily actively involve all five key players in a debit card transaction. That is (1) card issuer; (2) card holder; (3) merchant; (4) acquirer; (5) card associations. The existing non-standardized approach is a mash-up of active players involvement sometimes while some passive players are left beholding to others sporadically. The result is a disproportionate cost of transaction fraud absorbed inapposite to who should be held liable. The chart below depicts how both **BFR and merchant blocking uniquely actively involves all five key players and thus is a materially more effective** available and economical means by which fraud may be reduced on a cost/benefit analysis. When BFR is compared against merchant blocking, we find that merchant blocking's effectiveness is bifurcated. The first prong depends on transaction monitoring which as we will see below is a diminishingly flawed technology. The second prong depends on issuer ceiling limits and pre established parameters and is materially more effective. The metrics are difficult to discern as a consumer advocate. However issuer limits typically leads to a decline. Conversely transaction monitoring may lead to either a decline or card capture. It may also be appreciated that to the extent that transaction monitoring is involved in merchant blocking that it may necessarily lead to false positives. This equates to no-sale to the merchant and possible loss of consumer relationships for the issuer. Conversely BFR

is not rooted in buying pattern habits which is considered a thing. In fact BFR never authenticates the thing, it authenticates the person. This is an important distinction.

It may be compared to airport image scanners focusing on a thing e.g. shoes, underwear; as opposed to the "Global Entry Program" which focuses on people and is rooted in intelligence gathering. People should be the focus during debit card authentication and not a thing. The final adjustment fraud prevention activity cost must necessarily and actively involve all five key players along the value chain and should incentivize focusing on people and not the thing. Anything short of that sends the wrong message to the industry and the right message to the fraudsters.

MASHUP OF 5 KEY PLAYERS ROLE IN AUTHENTICATION STEP

Authentication Tool	Type of Fraud	Card Issuer	Card Holder	Merchant	Acquirer	Card Association
Biometric Facial Recognition	Zero	X	X	X	X	X
Merchant Blocking	Zero	X	X	X	X	X
PIN	Skimming[1] or cloning	X	X	O	O	O
Signature	Unable to [2] match/worn	X	X	X	O	O
EMV Chip	Reverse Engineer	X	O	X [3]	X (if issuer is offline)	X

[1] **PIN** – presumes card holder PIN customization. The threat vector lies at the merchant's POS or ATM when white plastic or counterfeit cards are used as the type of fraud.

[2] **Signature** – Merchants cannot request State Driver's License to match signatures. Furthermore it may require handwriting experts. Finally many signatures are either worn from water damage or similar.

[3] **EMV Chip** Merchant – presumes merchant has expensed for hardware upgrade to read chip. Many merchants resist this added expense. Acquirer is considered active particularly if issuer is unreachable or offline for authentication. The Chip also fails to prevent fraudulent new accounts opened in victim's names. In other words the card holder is not actively involved.

Card Activation	Mail Intercept Fraud	X	X	O	O	O
Phone Back	Out-of-Band[4]	X	X	O	O	O
RSA Tokens or Dynamic Data	Algorithm stolen[5]	X	X	O	O	O
Transaction Monitoring or Neural Ntwks	Patterns diminish[6]	X	O	X	O	O

Key: X – active involvement
O – passive or no involvement at all

Note: Other fraud tools such as CCV2, AVS, Firewall, software, and similar are to insignificantly effective to address relative to the sophisticated debit card savvy hacker and impersonator in the 21st Century. For example, there are social engineering techniques employed by thieves by pilfering Facebook account data. Transaction monitoring cannot prevent this type of fraud, but BFR can.

THE FINAL RULE ADJUSTMENT SOLUTION

There are two possible solutions to incentivize that all five key players are actively involved in fraud prevention activities and costs.

One is that the Board should "invoke such other factors as the Board considers appropriate" and therefore include the (0.4) four cents costs of BFR into the base of the interchange fee similar to transaction monitoring. Like transaction monitoring, BFR, assist in the authentication process by providing information to the issuer BEFORE the issuer decides to approve or decline the transaction. Additionally, BFR goes a step further by providing information to the merchant at the point of interaction BEFORE the merchant decides to approve or decline the transaction. As stated earlier BFR actively involves the card holder, acquirer, and card associations. Issuers

[4] **Phone Back** – Out of band refers to a spoofed phone number that actually calls back the thief.

[5] **RSA Tokens or Dynamic Data** – Remote Access Trojans (RAT) via a flash object embedded in an excel spreadsheet exposed many of Secure-ID`s customers costing issuers and card holders hundreds of millions of dollars. Acquirers, merchants, and the card associations may not have been directly affected.

[6] **Transaction Monitoring** – The most reported tool in the Board's survey which forms the basis of the adjustment inherent flaw is that the algorithm that the neural network is built upon becomes inherently less responsive and diminished as thieves adjust their pattern of the victims spending habits either by surveillance or as seen on the victim`s billing statements. This results in a diminished return on investment for the issuer. It also fails to actively involve all five key players in preventing debit card fraud.

may monitor transactions through the use of biometric facial recognition via declines and approvals from the merchant's systems. This bi-lateral communication is an important distinction not found in neural networks. It is however found in merchant blocking. In other words there is a specific transaction code that is reported by merchants back to issuer due to merchant blocking. BFR as advanced in this white paper is as integral to the authentication decision as confirming that a card is valid and authenticating the person and not the thing. In this suggested solution, the issuer should only claim the adjustment, once they actually deploy biometric facial recognition.

A second solution might be to decouple the 0.7 cents found in the flawed transaction monitoring authentication tool that comprises the base of the interchange fee in its current state. Once decoupled then append it to the fraud adjustment final rule along with the four cents totaling 3.3 cents (4.0 – 0.7 = 3.3). In that scenario, the issuer could only claim the full amount, if they actually deployed BFR. Alternatively they could claim 0.7 cents if they merely stayed with merchant blocking. Anything less than involving all 5 key players equals one cent.

WHY TRANSACTION MONITORING IS FLAWED

Transaction monitoring in and of itself is inherently flawed and should NOT be incentivized. Pattern matching and associative memory of debit card holder's buying pattern (the thing) need only be duplicated by dumpster diving for a billing statement or via surveillance of the victim's buying habits. The neural network learns what it is taught. Garbage in-garbage out. Thieves know this. Over a five year period the return on investment of the quality of scores leading up to multiple false positives inside a neural networks diminishes by sixty six percent (66%) according to entities familiar with the subject. This would explain why debit card fraud continues to

increase in light of transaction monitoring as the most reported security tool in the Board's survey. This is, by definition, why we are having this discussion in the first place.

Finally as stated on page 170 of the draft the cost of research and development of new authentication methods [such as biometric facial recognition] would be considered in the fraud-prevention adjustment, but would not be a cost that is specific to a particular electronic debit transaction. We support the Board's position here.

In either scenario, the objective should be to incentivize that all five key players actively participate in fraud prevention by way of authentication such as currently found in merchant blocking grounded in issuer limits as well as in BFR's role to detect, prevent, and eliminate fraudulent electronic debit transactions at the authentication step.

OTHER NOTABLE ISSUES REGARDING THE ONE CENTS

It is noteworthy that 46% of total transactions were not reported by networks that decided against transaction monitoring perhaps due to the diminished ROI, and thus those issuers are disproportionately prejudiced. The writer understands that the Board took the mean average from the survey.

The retrogressive one cents approach also fails to adjust for merchant's fraud prevention costs such as unilateral and non-ubiquitous fraud risk management systems with manual or automated review processes, analysis of IP address, and other endpoint information.

Thus, merchants are still being hit twice; once, by paying directly for their own fraud prevention measures, and secondly, by subsidizing the issuer's costs by way of this adjustment while still bearing the lion's share of the liability. The Board is urged to remain cognizant that

this interchange rule stems from the MasterMoney v Walmart, Safeway, Sears litigation that was presided over by Judge John Gleeson of the Brooklyn Federal District Court here in New York City on or about 1998. This rule may have also gained steam from the European Union's ruling held by Anti-Competition Commissioner, Nellie kroes of Brussels. Either way, this double hit to merchants in the current interim rule may rise to a level of what constitutes "reasonable recovery" and may require that the Board consider "such other factors as the Board considers appropriate" to prevent administrative legal costs, juror fees, mileage reimbursements, and inevitable appeals for many many years to come all over again, if the Board fails to balance this out correctly this time around. The writer understands that the Board has focused the interim adjustment solely on issuers. However, the Board may elect to invoke "other factors it considers appropriate". Such as the extent to which the occurrence of fraud depends on whether the authentication is materially more effective due to active involvement of all five key players at the authentication step. Consideration may also be revisited as to the fraud prevention and data-security costs expended by *each or all* players.

On a separate yet related matter, the writer is in favor of consumer reward programs advanced by either issuer and/or merchant in favor of a materially more effective technological fraud prevention activity as found in biometric facial recognition. (see draft page 370). Issuers currently may specify or promote use of a particular technology or method such as the flawed dynamic data to authenticate a card holder at the point-of-interaction. Issuers may also use expanded parameters for special promotional programs. The same should hold true for Biometrics Facial Recognition. (see draft page 379).

The writer is also in favor of a consistent certification process for card issuers that actively involve all five key players. Card associations could set the compliance standards to be implemented by the issuers.

The language of the Board's request for comments is good. It necessarily speaks to a specific audience versed in the subject matter and nomenclature. It was at times a bit redundant, but the subject involves a complex four-party cyclical process that was written under a significant time constraint. Overall this writer gives it a passing grade all things being equal.

SUMMARY

Biometric Facial Recognition represents a comprehensive fraud prevention and detection system available today. Its effectiveness is deeply rooted in active involvement of all five key players during a debit card transaction. The Board is urged to incentivize biometric facial recognition. The Board is urged to incentivize fraud prevention tools that necessarily include all five key players. Fraud prevention must necessarily focus on people and not a thing. The final rule may include the full four cent adjustment incurred as the total cost to issuer. Alternatively, the final rule may include three point three cents adjustment once the flawed neural network is decoupled from the base interchange fee. In either instance the cost should be fully recaptured by issuer once the technology is deployed.

ABOUT US

George Cox is CEO of www.HeadsUp.cc, a cyber security firm in Harlem U.S.A. that is currently operating in the CONUS and the Caribbean. The firm specializes in patented pending Point of Interaction transaction security and facial biometrics during card transactions. An

honorably discharged United States Air Force Veteran and inventor, he is also a network engineer and certified ethical hacker who earned an academic scholarship in banking and revolving credit 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 in Greensboro, North Carolina. He may be reached for comments via www.headsup.cc

Thank You Kindly,

George Cox, CEO

Disclaimer: The use of corporate names of MasterMoney, Walmart, Safeway, Sears, EuroPay, MasterCard, Visa, Facebook, Smart Phone and other well known established business names are the sole property of their shareholders and all rights are retained by those parties. Any mention of them in this comment is solely to draw the Board's attention to the current state of the environment that HeadsUp and other consumer advocates work within on a daily basis.