Fair Isaac Corporation
901 Marquette Avenue, Suite 3200
Minneapolis, MN 55402 USA
T 612 758 5200
F 612 758 5201
www.fico.com

Make every decision count.™

February 22, 2011

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW.
Washington, DC 20551.
SENT by email: regs.comments@federalreserve.gov.

RE: Debit Card Interchange Fees and Routing (New Regulation II)
Docket No. R–1404 and RIN No. 7100 AD63

Fair Isaac Corporation, dba FICO, respectfully submits these comments in response to the Federal Reserve Board's request for comment on possible frameworks for an adjustment to interchange fees for fraud-prevention costs (*Federal Register* / Vol. 75, No. 248 / Tuesday, December 28, 2010 / Proposed Rules).

About FICO

Founded in 1956, Fair Isaac (FICO) is a leading provider of credit scoring, decision management, fraud detection and credit risk score services. Our primary focus as a company is advanced analytics and decision management technology, and our efforts are primarily focused on the financial services sector. Our applications enable faster, more accurate and more coordinated decisions in order to enable more profitable and predictable customer interactions across the customer lifecycle. Key application areas for FICO in financial services are:

- Customer acquisition and marketing
- Originations and account underwriting
- Customer management
- Collections and recoveries
- Fraud detection and prevention

FICO has been a leader in fraud management pioneering neural network models, establishing the Fraud Consortium and real-time profiling techniques long before our first version of Falcon Fraud Manager became available in 1992. Falcon Fraud Manager is used by 17 of the 20 largest global card issuers and protects over 2.2 billion debit and credit payment cards globally. The expanding use of Falcon Fraud Manager over the last 20 years has reduced the basis points of card fraud losses in the US by 70%. The Falcon Fraud Manager and FICO Fraud Consultants in combination have helped thousands of financial institutions mitigate billions of dollars in card fraud losses.

FICO's focus is on developing analytic solutions to help issuers identify changing fraud patterns, and in rapid fashion, prevent fraud losses—in most cases by greater than 50%. FICO fraud protection solutions today give issuers the backing of the latest technology, sophisticated analytics and the largest fraud consortium database in the world.

The Board's Request For Comment

The Board's proposal requested comment on two general approaches to the fraud prevention adjustment framework and asked several questions related to the two alternatives.

Technology-specific approach. One approach to an adjustment for fraud prevention costs would be to allow issuers to recover costs incurred for implementing major innovations that would likely result in substantial reductions in fraud losses. This approach would establish technology specific standards that an issuer must meet to be eligible to receive the adjustment to the interchange fee. Under this approach, the Board would identify the paradigm-shifting technology(ies) that would reduce debit card fraud in a cost-effective manner. The adjustment would be set to reimburse the issuer for some or all of the costs associated with implementing the new technology, perhaps up to a cap; therefore, covered issuers and the Board would need to estimate the costs of implementing the new technology in order to set the adjustment correctly. Industry representatives have highlighted several fraud-prevention technologies or activities, such as end-to-end encryption, tokenization, chip and PIN, and the use of dynamic data that they believe have the potential to substantially reduce fraud losses. These technologies are not broadly used in the United States at this time . . . The drawback of adopting technology-specific standards is the risk that it would cause issuers to under invest in other innovative new technologies, not included in the Board's standards, that may be more effective and less costly than those identified in the standards.

Non-prescriptive approach. The second approach focuses on reasonably necessary steps for an issuer to maintain an effective fraud prevention program, but would not prescribe specific technologies that must be employed as part of the program. This approach would be to establish a more general standard that an issuer must meet to be eligible to receive an adjustment for fraud-prevention costs. Such a standard could require issuers to take steps reasonably necessary to maintain an effective fraud-prevention program but not prescribe specific technologies that must be employed as part of the program. This approach would ensure that the Board's standards give flexibility in responding to emerging and changing fraud risks. Under this approach, the adjustment would be set to reimburse the issuer for some or all of the costs of its current fraud-prevention and data-security activities and of research and development for new fraud-prevention techniques, perhaps up to a cap. This approach would shift some or all of the issuers' ongoing fraud-prevention costs to merchants, even though many merchants already bear substantial card-related fraud-prevention costs, particularly for signature debit transactions. Such a shift in cost provides issuers with additional incentives to invest in fraud-prevention measures. Financial institutions make investments today, however, to reduce the risk of fraud in non-card forms of payment, without reimbursement of those costs from the counterparty to the payment.

The Dimensions of Fraud

FICO believes the discussion must begin with an understanding of the dimensions of fraud. There are many kinds of fraud, and there are solutions, though not necessarily efficient and cost effective solutions, to each. Nevertheless, attacking the multi-dimensional problem of fraud is complicated, and the solutions vary depending on the nature of the company and its business, and the number of customers or the amount of customer data it holds. For example, preventing credit card data from being hacked in merchant databases can be accomplished by the merchant implementing tokenization technologies. End to end encryption (E2E) can be used to stop malware on a computer network connection sniffing for card data. Chip & PIN (EMV) technology can be used to reduce skimming fraud in face-to-face transactions. Each of these fraud prevention technologies can be used as an incremental upgrade to target specific weaknesses in the payment system criminals have compromised over the past decade or more.

Contributing to the complexity of finding solutions to fraud is that there is an important difference between fraud *prevention* and fraud *detection*. Fraud prevention is focused on identifying and reducing fraud up front. Prevention can include checking a consumer's history of account use at other financial institutions prior to giving a consumer an account with a debit card. A financial institution can prevent a potential first party (customer perpetrated) fraudulent account opening by denying the application all together based on past behavior. This "solution" would prevent a potential fraud loss, but if the consumer had been adversely affected by the economic crisis, and were looking to re-establish herself, denying credit might not be the best solution for the financial institution or the customer. In fact, the consumer may turn into a good and profitable customer for the financial institution. Fraud prevention is not guaranteed at the other end of the risk spectrum either, where even a good customer is susceptible to a third party criminal stealing information that can be used fraudulently creating a loss for the financial institution and consumer impact. The amount and type of fraud prevention activity that is ideal for a company depends on many factors, including the company's risk tolerance, prior fraud experience, financial condition, and management strategy for revenue and growth.

A better way to manage the fraud risk on this consumer's account may be to monitor the behavior on the account to *detect* fraudulent behavior. This is where predictive analytics, coupled with real time transaction monitoring, can detect fraudulent behavior as it happens. These solutions also adapt to the criminals' changing behavior over time, which is evolving rapidly, irrespective of the technical hardware

infrastructure used to prevent fraud. Detection is a component of prevention, whether the fraud is perpetrated by the actual customer (first party fraud) or by a criminal stealing access information and creating a fraudulent transaction (third party fraud). Both prevention and detection technologies are expensive, but both are necessary because not investing in these technologies would be catastrophic.

Detection of Fraud. Debit card issuers are uniquely positioned to understand their customer's behavior and the risk of each transaction. Monitoring transaction activity requires analyzing transactions in real time and providing an approve / decline decision prior to completion of the transaction. This decision is more complex than simply determining if there are enough funds to support the transaction. The decision is based on the cardholder's historical usage profile, non-monetary transaction behavior (such as a change of address), and known criminal transaction patterns. Further data points can be incorporated into the decision such as the balance in the account overall, the risk score derived when the customer applied for the account, and the risk of the account going into collections. Each of these components can be used to determine the level of risk the transaction represents.

Understanding the known behavior patterns of customers and criminals and assigning a risk level prior to funds moving (the riskiest part of a transaction) is crucial to the detection of fraud. Application fraud, using a synthetic identity, stolen identity or a consumer's actual identity (first party fraud), is another dimension of fraud that financial institutions have to manage. There are situations where criminals open demand deposit accounts with the intent to deposit bad checks and withdraw the funds via ATM or make card purchases prior to the checks being returned. Criminals will also purchase accounts from 'good' customers and perpetrate these frauds.

Investing in Fraud Prevention and Detection. Financial institutions have to deal with global criminal networks that steal money from customer accounts through the use of payment card data which results in money laundering of proceeds around the world and supports all types of crimes from drugs to terrorism. Debit card fraud is sometimes perpetrated by lone individuals, but often by highly organized criminals. Many of these criminals use sophisticated hacking techniques to steal card data and sell it around the world. The internet is used as a way for criminals to connect to each other, trade information and build their 'businesses'. These card frauds are used as a source of revenue to support other crimes that are generally much more heinous and violent than card fraud and, in some cases, support terrorist activities. As criminals monetize the data, they invest more to expand their operations. The ease and relative safety of these operations breed more criminals. Most times, the compromised data is unknown until the fraudulent activity starts and law enforcement is not equipped with the resources, know-how, and international connections to control it.

Any reduction in fraud detection and prevention activity will create a vacuum that will be immediately backfilled with extended criminal activity and losses to society. A system that does not invest in the appropriate controls to manage fraud will have it grow to uncontrollable levels; a case in point is the level of healthcare fraud and abuse in the US. Another example is the experience of the U.S. Department of Defense, which implemented an analytic application to identify the fraud and abuse of procurement cards by the employee-cardholders' themselves. Creating and maintaining the "appropriate controls" requires a long-term commitment by the industry and government. Companies must invest in research and development, monitoring fraud activity, putting safeguards in place, assessing the effectiveness of those controls, and then starting over again when the fraud environment changes again. The entire economy benefits when fraudsters are foiled, but that battle will be extensive, expensive, and ongoing.

The Board's Specific Questions

1. Should the Board adopt technology-specific standards or non-prescriptive standards that an issuer must meet in order to be eligible to receive an adjustment to its interchange fee? What are the benefits and drawbacks of each approach? Are there other approaches to establishing the adjustment standards that the Board should consider?

FICO: The Board should adopt non-prescriptive standards for management of fraud detection and prevention. Issuers have a broad range of tools and approaches that can be used to manage the ever changing fraud landscape. Issuers should be incented to use the most robust form of fraud detection to reduce fraud losses, rather than be incented to make a mandated technology change that is only effective for a specific 'dimension' of fraud and will eventually be surpassed by another significant investment once the technology is compromised.

This same question has been asked repeatedly with respect to standards for data protection since the Gramm-Leach-Bliley Act was enacted in 1999. The course chosen by federal regulators, which has been wise and effective, has been to require "reasonable" standards of data security. This non-prescriptive approach requires companies to adhere to ever-evolving industry and government best practices. The approach has allowed regulators to have flexibility to require appropriate standards that vary among companies, based on the size and sophistication of the business, the amount and sensitivity of the data, and the cost of the technology. Requiring companies to adhere to industry best practices also imposes, without having to set prescriptive rules, an ever-increasing duty on the companies to increase their commitment to safeguarding data and preventing fraud and identity theft.

Any technology specific standard will eventually be outdated, which requires the Board to continue to revisit the issue and make mandates that may or may not be in the best interests of the industry and consumers. This obsolescence factor even applies to state-of-the-art data protection standards such as PCI DSS, which are continually updated over time. In fact, several entities that were determined to be PCI compliant suffered some of the largest data breaches to date. PCI compliance is a point in time and any changes to a system, intentional or not, may result in a weakness that is exploited. Again, fraud detection, the decision at authorization, is the last chance to understand if a criminal or the actual customer is initiating the transaction.

Even if the Board could anticipate the evolving needs to combat fraud, changes to the technology-specific standards would take valuable time, and the financial services industry would be vulnerable during the time it takes the Board to revise the standards. A non-prescriptive, layered security approach offers the best detection and prevention capabilities to meet current and emerging fraud scenarios over time. This allows for flexibility to implement the latest technologies and best practices that meet the changing fraud schemes.

The most preeminent magnetic stripe replacement technology, Chip & PIN (also known as EMV), was developed in the 1990's. This technology decreases fraud loss in card present transactions (when it is not falling back to the magnetic stripe) however in markets where it has been implemented, the rate of card not present (CNP) and cross border card present counterfeit fraud losses have increased substantially. The fraud problem can be imagined as a balloon; when squeezed in one spot, it expands in another. Nevertheless, there are estimates that it will take as many as 10 years to fully implement Chip & PIN in the US. By this time the technology will be over 25 years old. A major investment in this particular technology will reduce investment in newer more efficient methods such as contactless and mobile technologies which have similar fraud reduction techniques and enable a broader and more efficient usage profile, particularly for smaller purchases and mass transit.

Another example of a flexibility of a non-prescriptive recommendation for fraud reduction is multi-factor authentication for online banking. The FFIEC was in a similar situation in 2005 when they offered guidance to financial institutions requiring them to implement multi factor authentication for on-line banking sites. The FFIEC did not require a technology specific solution, just one that would require more authentication than just a single factor such as a password. Financial institutions were then able to choose from competing vendors or in-house solutions to deal with the problem. As expected, the criminals were able to circumvent the technology put in place with man-in-the-middle attacks and man-in-the-browser attacks.

The principal reason not to use the prescriptive approach is that, regardless of the technology put in place, criminals will work their way around the technology and the prescriptive standards will need to be changed to deal with changing criminal attacks. Once the financial institutions adapt to any particular scheme, the criminals will again innovate their methods. This requires the adaptability of fraud prevention and detection efforts. Financial institutions are now looking to add predictive analytics to monitor the account behavior to identify suspicious transactions so when a criminal is able to take over an account, the risk of the transaction is identified prior to the money moving.

2. If the Board adopts technology-specific standards, what technology or technologies should be required? What types of debit-card fraud would each technology be effective at substantially reducing? How should the Board assess the likely effectiveness of each fraud prevention technology and its cost effectiveness? How could the standards be developed to encourage innovation in future technologies that are not specifically mentioned?

FICO: If the Board adopts technology-specific standards, the Board must choose a "soft" technical solution, rather than a "hard" solution. A 'hard' technology solution is one which is designed to deal with a specific technical or hardware standard. The hard solution seems to stand on its own to solve a specific fraud problem; some might call or consider it a silver bullet to stopping fraud. A hard solution requires significant investment from all parties and limits the flexibility of responding to an ever changing environment along with the unintended consequences or repercussions of the decision. An example of a hard solution is Chip & PIN (EMV), as it requires across the board investment to upgrade all payment terminals and all payment cards.

By contrast, a soft solution is adaptable to changing criminal behavior patterns and compromise methods which allow the issuer to manage fraud in systematic way. The ability to adjust to the criminals' behavior and understand your customers' behavior is critical in identifying fraudulent transactions during the authorization process. This is the strongest method of fraud prevention and detection and is the last line of defense before the money moves. Regardless of the hardware used in a transaction processing environment, predictive analytics that calculate and adapt to changing consumer behavior patterns with changing criminal modus operandi provide the maximum level of protection to a payment account or vehicle, such as a payment card.

Even the most advanced fraud prevention implementations will require a layer of fraud detection to manage shifting criminal attacks. When we build 10 foot walls of hard technology, criminals will develop a 12 foot ladder. An example of this is the Chip & PIN attacks that Ross Anderson, Professor at Cambridge University of Security Engineering, has demonstrated a technique to defeat the PIN verification process on a Chip & PIN card. This is further evidenced by the fact that Chip & PIN card issuers continue to use predictive analytics coupled with real time transaction monitoring to detect fraudulent behavior as it happens on the payment cards they issue.

Summary

The best prevention and detection tools will still not eliminate fraud losses. The cost of fraud losses will be borne by the financial system that makes debit cards possible. The financial system stands to gain if the players in the system can reduce the fraud losses that will never go away. The costs of reasonable fraud prevention and fraud detection should be underwritten by the people who benefit from a reduction in fraud costs. If financial institutions invest wisely in fraud prevention and fraud detection technologies, the resulting reduction in fraud costs helps the entire financial system: it benefits the financial institution, the network, and the consumer.

FICO urges the Board to refrain from prescribing solutions that would limit companies' abilities to respond to the ever-changing patterns of criminal behavior, or incent companies not to invest in valuable fraud prevention and fraud detection technologies.

Sincerely,

Michael Urban
Senior Director, Product Management
FICO