Debit Card Fraud:
The Impact of Proposed Regulations
on the Food Retailing Industry

Prepared for the Food Marketing Institute

By

Orzechowski & Walker

February 2012

Debit Card Fraud: The Impact of Proposed Regulations on the Food Retailing Industry

Executive Summary

There are nearly 520 million debit cards in circulation in the United States. Last year, $1.38 trillion in transactions -- 30 percent of all retail sales in America in dollar terms -- were made using debit cards.

Fifty-nine percent of debit card transactions in the United States are verified using the consumer's signature. These Signature debit transactions are much less secure than those verified through the use of a Personal Identification Number, or PIN. In fact, 85 percent of all fraudulent debit transactions involve Signature debit. Signature debit transactions were responsible for $1.15 billion of the $1.35 billion in total debit fraud losses.

Despite the higher frequency of fraud, banks have historically encouraged consumers to use Signature debit cards, which are more profitable for banks than PIN debit cards. Banks can make an extra $4.10 in profit per every $1,000 in transactions when consumers use Signature debit instead of PIN debit.

Based on numbers from the Federal Reserve, it is estimated that retailers lose $580.5 million on debit fraud. They also spend $6.47 billion annually on credit and debit card fraud prevention systems.[1] One reason for this investment is that merchants share in the cost of these losses and have an incentive to minimize them.

Were issuers and consumers to adopt more secure PIN debit, or move toward the more reliable systems currently used in Europe, the costs from fraud loss could be reduced dramatically.

Level and Types of Debit Transactions

Debit card transactions have been growing at a tremendous rate over the past decade, far outstripping the growth in credit card transactions.[2] According to Visa and MasterCard, there are nearly 520 million debit cards currently in circulation in the United States.[3] Over 37 billion debit card transactions were made last year totaling $1.38 trillion,[4] representing almost 30 percent of all retail sales in America (in dollar terms).[5]

Debit card transactions are currently verified in two ways; with the cardholder's signature (Signature debit), or through the use of a Personal Identification Number, or PIN (PIN debit).

---

1 See Table 3 for details.

2 Pilon, Mary, *Debit Cards Overtake Credit Cards*. The Wallet, Wall Street Journal Blog, August 6, 2009.

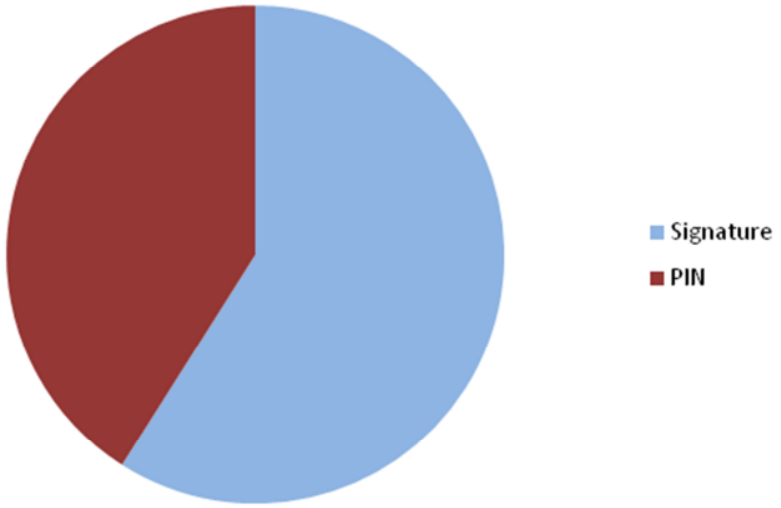
3 As cited in, Woolsey, Ben and Matt Schulz, *Credit Card Statistics, Industry facts, Debt Statistics*, Credit Cards.com, www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php#Debit-cards

4 Ibid.

5 U.S. Department of Commerce, Bureau of the Census, *Advance Monthly Sales for Retail and Food Services, 2010*, on-line at: www.census.gov/econ/currentdata/marts/?programCode=MARTS&yearStart=2010&yearEnd=2010&categoryCode%5B%5D=44X72&dataTypeCode=SM&geoLevelCode=US&adjusted=0&notadjusted=0&notadjusted=1&errorData=0

Signature debit transactions are processed over the same network as regular credit card transactions, while PIN debit is processed over separate networks. As such, PIN debit transactions happen in real-time, while Signature debit transactions involve a two-step process. First there is an authorization, and then a settlement where the money is transferred. Of the $1.38 trillion in purchases, about 59 percent were Signature debit (totaling $816 billion) while 41 percent ($567 billion) were PIN debit transactions.[6] (See Figure 1)

Figure 1
Total Volume of All U.S. Debit Transactions (2010)



Banks in the United States promote the use of less secure Signature debit transactions, often offering incentives for customers to switch from PIN debit to Signature debit.[7] While Signature debit is not as safe as PIN debit, merchants bear more of the cost of fraud, so liability shifts away from issuers. More importantly, card issuers have historically earned significantly more revenue from Signature debit transactions. As one security analyst notes, "PIN is actually more secure, but PIN does not generate as much revenue to the bank."[8]

As Table 1 on the following page shows, even though issuers face higher costs for Signature debit, this is more than made up for by the $7.50 in additional revenues per $1,000 worth of

6 Op cit Woolsey. Also see: 12 CFR Part 235, *Debit Card Interchange Fees and Routing: Proposed Rule*, Federal Register, Vol. 75, No. 248, Dec., 28, 2010, and *The Nilson Report*, Issue 970, April 2011, page 9, The Nilson Report, Carpinteria, California.

7 For example, Citibank customers receive 1 rewards point for every $2 purchase made using signature debit, while it takes $3 in PIN purchases to earn the same reward. TD Bank has offered programs that reward customers $50 for debit purchases made using signature authentication. See: Lepro, Sara, *Counterintuitive Pitch for Higher-Fee Debit Category.*" American Banker, April 21, 2010, at: www.americanbanker.com/search/index.html?zkDo=search&frommonth=02&fromday=26&fromyear=2010&tomonth=08&today=26&toyear=2011&publication=all_articles&query=JP+Morgan+Chase+tells+customers+signatures+are+safer+than+PINS&x=31&y=10

8 Ibid. The quote is from Adil Moussa, an analyst for Aite Group.

transactions that they collect.[9]

Table 1
Issuers' Profit and Loss Analysis for Debit Card Transactions – Signature vs. PIN

($ Per $1,000 in transactions)	Signature	PIN	Difference
Revenues	$14.20	$6.70	$7.50
Interchange Fees	$14.20	$6.50	$7.70
Account Fees		$0.20	($0.20)
Costs	$4.50	$1.10	$3.40
Network Fees	$1.70	$0.50	$1.20
Processing Fees	$0.80	$0.20	$0.60
Rewards Programs	$1.20	$0.00	$1.20
Fraud	$0.80	$0.40	$0.40
Profit Margin to Issuing Banks	$9.70	$5.60	$4.10

Source of Data: Pulse

Issuing banks have another, very powerful incentive for continuing to perpetuate the use of riskier, signature debit transactions; the issue of "float". As a general assumption, Signature debit transactions can take between 2-3 days to clear the cardholder's account, which means that issuing banks have the use of those funds during the payment clearing window.[10] This allows banks to earn as much as $17.2 million in additional interest revenue that would not be obtained had cardholders used PIN debit cards instead.[11] The perverse incentive for banks to encourage the use of Signature debit transactions conflicts with the Federal Reserve's initiative to speed up the payment system and ultimately eliminate float.[12]

On top of the fees that issuers have traditionally generated from interchange fees on merchants and from interest on their float, some major financial institutions are beginning to charge card holders for the "privilege" of accessing their own funds. One of the nation's largest banks will be implementing a $3 per month debit card fee to cardholders.[13] More may follow suit. If this were applied to the 520 million cards outstanding, that would equal $18.7 billion annually.

The lack of proper incentives and the enhanced revenues from Signature debit leads issuers to encourage Signature debit. The result of this encouragement – the disproportionate use of Signature debit in the U.S. – makes reducing debit card fraud difficult.[14] Most other

9 *2010 Debit Issuer Study*, Pulse©, A Division of the Discover Network, 2011.

10 Payment Information Center, at www.paymentinfocenter.com/creditcard/.

11 Dividing the annual volume of signature debit transactions ($837.0 billion) by 365 yields an average volume of transactions of $2.2 billion per day. Interest of 25 basis points on $2.2 billion times 3 days would equate to $17.2 million.

12 See The National Automated Clearing House Association at: www.nacha.org/c/aboutus_History.cfm

13 *ABA Daily Newsbytes*, June 29, 2011.

14 Issuers' rationale for not switching is that their losses do not exceed the costs of the new technology, which would be about $3.2 billion, of which merchants would cover $2.6 billion, yet many (Kroger, Sears, Walgreens) are pushing to convert. See: *House of cards Why your accounts are vulnerable to thieves*, Consumer Reports, June, 2011.

industrialized countries are using EMV (Europay/Mastercard/Visa) PIN debit smart-cards that contain computer chips. These chips transmit encrypted data and a unique identifier that can change with each transaction. In addition to the encryption, the requirement that cardholders enter a PIN to authenticate the transactions makes EMV PIN much more secure than payment processes in the United States. This is because the chip authenticates that the card is real, while the requirement that a PIN is entered ensures that the card belongs to the person making the transaction. Total fraud losses dropped by 50 percent and card counterfeiting fell by 78 percent in the first year after banks in France introduced this technology back in 1992.[15] American issuers, on the other hand, are still using unencrypted magnetic stripes for card verification. The European Central Bank recommends that cards with magnetic stripes no longer be used.[16]

Estimated Levels of Debit Fraud

Because of the high level of Signature debit in the United States, fraudulent transactions are a problem for those merchants that accept debit cards. It is estimated that over 85 percent of the $1.35 billion in debit card fraud losses comes from Signature debit transactions.[17] (See Table 2). Slightly less than one percent of all debit card transactions nationwide were ultimately fraudulent.[18] While this level of fraud is not insignificant, it does not justify the Federal Reserve's interim fee to cover fraud losses.

Table 2
Fraudulent Debit Transactions by Type

	Total US Economy	Percent of Total
Signature Debit Fraud Losses	$1,150,000,000	85.19%
PIN Debit Fraud Losses	$ 200,000,000	14.81%
Total Fraud Losses	$1,350,000,000	100.00%
Losses Per Debit Card (Signature)	$ 2.21	
Losses Per Debit Card (PIN)	$ 0.38	

Source of Data: Federal Reserve, 12 CFR Part 235

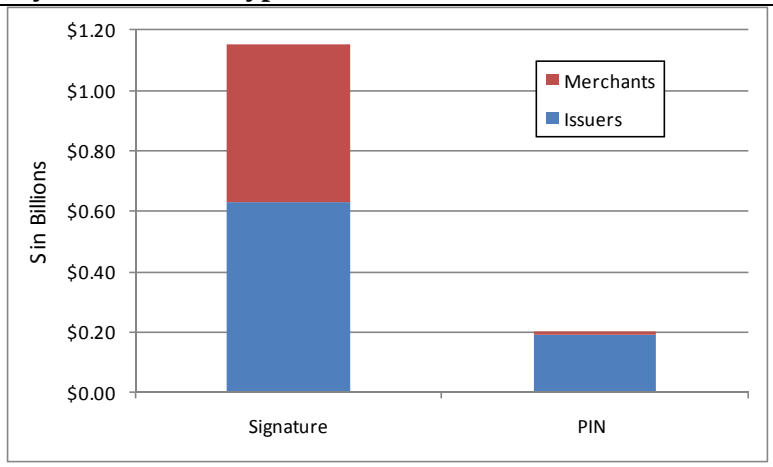
Issuers and merchants generally share the direct cost of fraud losses. The actual fraction of the loss depends on the type of transaction. According to data from the Federal Reserve, the loss from Signature debit transactions is generally split about evenly between merchants and issuers, while the losses from PIN debit transactions are predominantly borne by issuers.[19] (See Figure 2).

15 Ibid.
16 Ibid.
17 12 CFR Part 235, *Debit Card Interchange Fees and Routing: Proposed Rule*, Federal Register, Vol. 75, No. 248, Dec., 28, 2010.
18 Ibid.
19 Op. cit. 12 CFR. For PIN debit, issuers are liable for about 98 percent of fraud losses while merchants are charged back for about 4 percent. In the case of Signature debit, issuers are liable for about 55 percent of costs, while merchants are charged back for about 45 percent.

There is some rationale behind this difference. In the case of Signature debit transactions, the retailer has a key role to play, as it is the responsibility of the retailer to verify the identity of the purchaser by comparing the signature on the card with the signature on the receipt.[20] Overall, 55 percent of the direct cost of fraud from Signature debit is borne by the financial institutions and 45 percent by merchants.[21]

In the case of a PIN debit transaction, however, the responsibility largely lies with the financial institution. The PIN is entered by the purchaser, and if authenticated by the issuing bank, is authorized. As a result, 96 percent of the direct cost from fraud resulting from PIN debit transactions is borne by financial institutions. Consumers, the Visa/MasterCard networks and acquirers are generally held harmless due either to contractual or regulatory limitations on their liability.[22]

Figure 2
Incidence of Loss by Transaction Type



Source of Data: Federal Reserve, 12 CFR Part 235

These differences in both the magnitude and the liability for fraudulent debit card transactions permeate the entire structure of the industry in the United States, and have created both perverse incentives for card issuers to encourage Signature debit, while at the same time saddling merchants with a disproportionate share of the cost of fraud mitigation.

---

20 Even so, network rules prevent the retailer from denying a transaction simply because the signature on the receipt and the one on the card do not match.

21 Op. cit. 12 CFR

22 An acquiring bank (or acquirer) is the bank or financial institution that accepts credit and or debit card payments for products or services on behalf of a merchant. The cost of services performed by the acquiring bank are mostly passed through to the merchants. Note that consumers may be liable for $50 in fraudulent transactions if they report the compromise of the debit card within two business days after realizing that the card has been compromised. This liability increases to $500 if the loss after two but before 60 days. If a debit card is not reported lost of compromised for more than 60 days after the issuer mails the statement documenting the unauthorized use, the consumer may be responsible for the transactions. See: *Credit, ATM and Debit Cards: What to do if They're Lost or Stolen*, Federal Trade Commission, at: www.ftc.gov/bcp/edu/pubs/consumer/credit/cre04.shtm

Merchants are Responding to The Problem of Debit Fraud

Merchants have many reasons to prevent fraud beyond losses of revenue. Retailers spend large amounts of resources and effort to build a brand and establish brand loyalty. This includes protecting their customers from fraud and providing them with easy and secure ways to pay for products and services. For this reason, merchants have been enacting measures to prevent fraud for decades. In addition, the card networks, through the Payment Card Industry Council, have imposed new and costly rules on merchants (the Data Security Standards) that require expensive system upgrades. This means that the mere acceptance of debit cards requires the retailer to implement a variety of costly -- and largely unproven -- fraud prevention measures, including: [23]

- PCI Compliance: Merchants who accept credit or debit cards must ensure that they function in accordance with Payment Card Industry Data Security Standard (PCI DSS). This standard specifies controls around cardholder data to reduce debit and credit card fraud via its exposure.
- PCI Annual Maintenance: An annual compliance assessment with a certified PCI vendor is required for all merchants who accept credit and debit cards as a form of payment.
- In-store security cameras: Used to capture and validate card-presenter identity.
- Employee orientation, training and testing in PCI standards and compliance in fraud mitigation techniques.
- PIN-pads and PIN-pad compliant terminals: Used by merchants to validate Personal Identification Numbers. These terminals are not required if the merchant accepts only Signature debit.
- Real-Time Purchase Authentication: Including Internet transactions.
- Secure maintenance of historical payment data.

As Table 3 on the following page shows, the total cost of fraud (which includes both fraud prevention and losses due to fraudulent transactions) can be quite high.[24] Based on the 520

---

[23] See: *2009 LexisNexis® True Cost of Fraud Study*, conducted by Javelin Strategy & Research, 2009, *Grocery Industry Report on the Durbin Interchange Rulemaking*, Food Marketing Institute and National Grocers Association, 2010, *Stopping Data Cyberthieves in Their Tracks*, Delta Systems White Paper, July, 2010, 12 CFR Part 235, *Debit Card Interchange Fees and Routing: Proposed Rule*, Federal Register, Vol. 75, No. 248, Dec., 28, 2010. Retailers may also implement other security provisions, such as: End-to-end encryption; the replacement of sales terminals to comply with EMV smart-chip technology; rules-based filtering technology which restricts and/or blocks high risk transactions based upon specified criteria such as dollar amount, etc.; neural network fraud screening that calculates the probability of risk of transaction and calculates a score; real-time transaction tracking tools; and automated transaction scoring technology. It is important to note that while many of these measures may be required, most are unproven in their ability to actually reduce or prevent fraud.

[24] John Dunham and Associates Calculations. According to the Federal Reserve, the total annual cost of fraud is $1.35 billion (12 CFR Part 235). Of this, 57 percent is borne by issuers and 43 percent by merchants. Fraud prevention costs for issuers are estimated to be between 1.6 and 2.5-cents per transaction (12 CFR Part 235). To get the figures in the table, these costs are multiplied by an estimated 38 billion transactions (12 CFR Part 235). Spending on fraud prevention losses for merchants are based on data from the Food Marketing Institute. The mean estimate is the mathematical average of the prevention cost profiles of the largest and smallest retailers, applied to all retailers. Data are not available in enough detail to allow for the calculation of a weighted average, or industry average value. This includes the initial costs of compliance amortized over 5 years as well as annual costs. See: *Grocery Industry Report on the Durbin Interchange Rulemaking*, Food Marketing Institute and National Grocers Association, 2010.

million debit cards in circulation, this means that the average issuer faces an estimated $1.50 in fraud prevention costs per card, plus direct fraud losses of $1.48 per card. On the other hand, financial institutions generate about $118 in fees and other charges from each debit card that they issue, for an average estimate of net revenues of $115 per card. This implies a profit margin of over 97 percent before minimal operating costs are taken into account.[25] As for merchants, they face total costs from fraud prevention (and a very limited incidence of total fraud) averaging about $8 billion, or approximately $15.42 per card.[26] On top of these costs the average card creates about $87 in interchange expenses for the merchant.[27]

Table 3
Total Cost of Debit Card Fraud in All Retail Outlets by Liable Party

	Mean Estimate	Percent of Total
Costs Borne By Issuers		
Spending on Fraud Prevention	$ 779,000,000	9.71%
Actual Fraud Losses Incurred	$ 769,500,000	9.60%
Subtotal	$ 1,548,500,000	19.31%
Costs Borne by Merchants		
Spending on Fraud Prevention	$ 5,890,000,000	73.45%
Actual Fraud Losses Incurred	$ 580,500,000	7.24%
Subtotal	$ 6,470,500,000	80.69%
Total	$ 8,019,000,000	100.00%

Data Sources: Federal Reserve and Food Marketing Institute

Overall, the costs of fraud tend to be borne by merchants, even though these firms have only limited ability to either prevent or discourage fraud. As long as debit card issuers promote the use of the least secure technologies, and the requirements for accepting debit cards preclude merchants from denying transactions where signatures do not match, their ability to reduce fraud will be hampered. However, as the next section shows, by promoting the use of PIN debit transactions, the nation's food retailers have made significant strides to limit the opportunities for fraudulent transactions.

Impact of Debit Fraud on the Food Retailing Industry

According to Dun & Bradstreet there are nearly 328,500 food retailers in the United States.[28]

25 Op. cit., Pulse.

26 This is not to suggest that retailers gain no benefits from the use of debit cards. Among other things, debit cards are popular among retailers' customers; offering that payment option can increase customer loyalty.

27 Pulse Ibid. Interchange expenses are the transaction fees that merchants must pay to the Visa and MasterCard networks. Additionally, merchants who fail to comply and report a fraud incident to an issuer in a timely manner are subject to potential fines up to $500,000. See: *Visa PCI Fines/Fees and Data Breach Costs*, Visa USA Website – Risk Management, CISP, 8/31/2010.

28 Establishment employment is based directly on data provided to JDA by Dun & Bradstreet, Inc Zapdata system as of July 2011. Dun & Bradstreet data is recognized nationally as a premier source of micro

These range from 100,000 plus square foot hyper markets to small local bodegas. In addition to grocery stores and supermarkets, food retailers include a myriad of butchers, dairy stores, fruit and nut stands, candy stores and bakeries. These retailers generated $563 billion in sales in 2010, or 13 percent of total retail sales in the country. [29] Approximately 35 percent of these sales ($197 billion) were made using either Signature debit or PIN debit cards.[30] Table 4 displays data on food retailer transactions in 2010 in comparison to total U.S. retail sales.

Table 4
Food Retailer Transactions Compared to Total Retail Sales

($ in Billions)	Food Retailers	Total US Economy	Food Retailers as Percent of Total
Number of Retail Outlets	328,443	1,100,943	29.83%
Total Retail Sales	$563	$4,355	12.93%
Total Debit Card Transactions	$197	$1,383	14.24%
Signature Debit Transactions	$55	$816	6.76%
PIN Debit Transactions	$142	$567	25.02%

Source of Data: Dun & Bradstreet and Food Marketing Institute

Debit card transactions are critically important to the food industry as more and more consumers choose debit over credit, cash, and checks. Despite the prevalence of antiquated card technology in the United States, food retailers have been particularly effective at preventing fraud, in part by encouraging the use of PIN debit. Primary research conducted by the Food Marketing Institute (FMI) indicates that the average rate of claimed fraudulent transactions that are determined to be the responsibility of the merchant (and are therefore, charged back to the merchant's account as an actual loss) is less than one-one hundredth of one percent.[31] This is 98 percent lower than the level of debit card fraud (in terms of total percentage of retail sales) experienced in the general economy, and by non-food retailers. Part of this is due to the higher use of PIN debit, and part due to the fact that the larger food retailers in particular spend significant resources to ensure that they are not responsible for fraudulent transactions or chargebacks.

Based on this 0.001 percent figure, total charge-backs are estimated to be just $2.2 million.[32]

industry data. The D&B database contains information on over 15 million businesses in the United States. It is used extensively for credit reporting, and according to the vendor, encompasses about 98 percent of all business enterprises in the country.

29 *Supermarket Facts – Industry Overview 2010*, Food Marketing Institute, on-line at: www.fmi.org/facts_figs/?fuseaction=superfact, and *Debit-Card Use Overtakes Credit: Visa's Results Show Tilt Toward Paying It Now; What Does It Mean?* Wall Street Journal, May 1, 2009.

30 Calculations based on unpublished data from the Food Marketing Institute (FMI), FMI's *Supermarket Facts: Industry Overview 2010* online at http://www.fmi.org/facts_figs/?fuseaction=superfact., and FMI's *Annual Financial Review 2010 – 2011*, page 13.

31 See Food Marketing Institute, unpublished data, 2011. These data are based on a survey of FMI members. While the analysis is based on a small sample of retailers, these firms represent over 40 percent of total grocery sales, suggesting that the sample represents overall transactions and costs very well.

32 $197 billion in total transactions multiplied by 0.001 percent equals $2.2 million. Source: Food Marketing Institute, unpublished data, 2011.

(Table 5 on the following page). In other words, even though 12.93 percent of retail sales are made by food retailers, only 0.16 percent of fraudulent debit transactions that are charged back can be attributed to these stores. The low share of debit card losses in the food retailing industry compared to those experienced in the general economy can be attributed to the high percentage of food retailing transactions that involve PIN debit (See Figure 3).

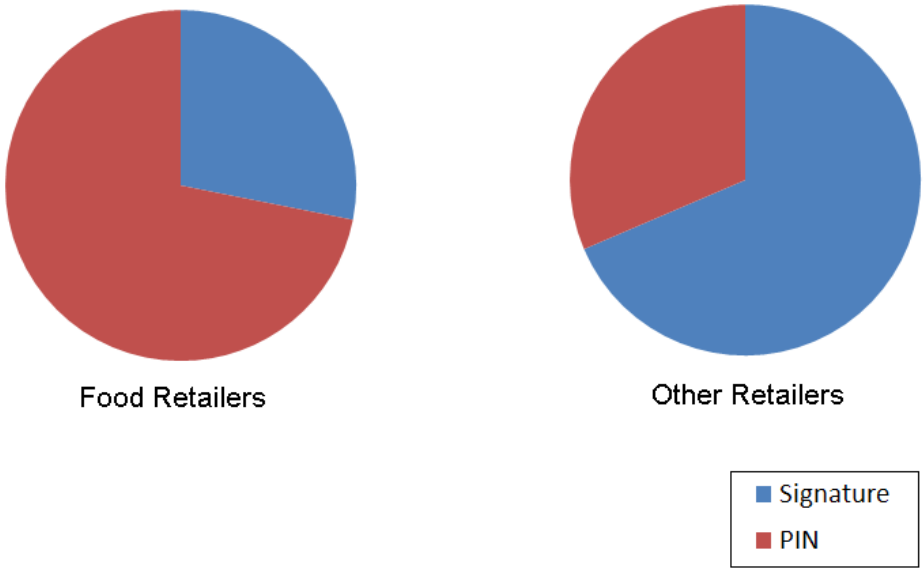
Table 5
Fraudulent Debit Transactions: U.S. Food Retailers vs. Total US Economy

	US Food Retailers	Total US Economy	Food Retailers as Percent of Total
Signature Fraud Losses	$2,167,477	$1,150,000,000	0.188%
PIN Fraud Losses	$1,331	$200,000,000	0.001%
Total Fraud Losses	$2,168,807	$1,350,000,000	0.161%

Source of Data: Food Marketing Institute unpublished data

Fraud as a share of sales volume is much higher for Internet, mail order, and telephone transactions than for point-of-sale merchants such as food retailers.[33] In the case of debit card transactions, card issuers even cite "data breaches and compromises" which take place at the network, not merchant level, as the major sources of fraud.[34]

Figure 3
Percentage of Transactions by Debit Card Type



[33] Op. Cit., Sullivan.
[34] Op. Cit. Pulse.

Despite a low fraud rate, food retailers are likely paying a disproportionate amount to prevent debit card fraud, especially considering that their customers predominately use a lower risk payment method (PIN debit). It is difficult to estimate the cost of fraud across the entire food retailing sector; however, if food retailers accepted debit cards at the same rate as other stores, they could be paying as much as $3.17 billion in fraud prevention costs, over 100 times what they actually lose from fraudulent transactions.[35]

Recent Federal Reserve Board Activities

In July 2010, President Obama signed into law the *Dodd-Frank Wall Street Reform and Consumer Protection Act* (Public Law-111-203). The bill granted the Federal Reserve Board authority to regulate interchange fees for covered financial institutions so that they are "reasonable and proportional to the cost incurred by the issuer with respect to the transaction." On June 29, 2011, the Board adopted an interim rule that capped fees at 21-cents per transaction, plus 5 basis points of the total transaction amount to account for debit-fraud losses. The Board also allowed issuers a 1-cent per transaction fraud prevention adjustment provided they meet certain criteria.[36]

The interim rule does not serve the ultimate purpose of preventing fraud. Issuers have profit incentive to continue to encourage and increase the use of less secure Signature debit cards. Issuing banks will continue to shift the burden of losses onto merchants, even as they are compensated on every transaction for potential fraud loss.

Merchants, who ultimately bear roughly half of the costs of these debit fraud losses and incur billions of dollars in fraud prevention costs, will not be similarly compensated. There is an additional disparity in the case of food retailing. The share of safer PIN-debit transactions is higher in food retailing than it is within the rest of the economy, and the loss from fraud is accordingly lower. Yet by paying 5 basis points for debit fraud losses, regardless of the transaction type, food retailers would be effectively subsidizing the cost of fraud that disproportionately takes place in other parts of the payment system..

Examples from abroad and from the United States' food retailing industry show that the problem of debit card fraud is not insurmountable. Smart-cards that combine computer chips with PINs are employed in most other parts of the world and are safer still.

A regulatory strategy designed to reduce debit fraud needs to take these findings into account. Rules that fail to adequately address these perverse incentives and ignore the systematic disparities between competing card technologies are unlikely to prevent the costs from debit card fraud from increasing. They will also impose unnecessary costs on merchants, like those in the food retailing industry, leading to higher prices and fewer jobs at a time of economic distress.

---

35 Based solely on the share of retail outlets.

36 Sidley Austin, LLP, *Federal Reserve Board Issues Final Rules on Debit Card Interchange Fees and Routing*, July 7, 2011. Online at http://m.sidley.com/federal-reserve-board-issues-final-rules-on-debit-card-interchange-fees-and-routing-07-07-2011/.