

THE INDEPENDENT

VOLUME 1, ISSUE 2

NOVEMBER 2011



Durbin Amendment/Federal Reserve Update

Finalizing Durbin

The Federal Reserve released its final ruling on interchange on June 29, 2011, a couple months late. Retailers and merchants were displeased with the ruling as the final rate is roughly twice the proposed rate. The banks were successful in lobbying the Fed to include several costs not included in the proposal rate. Additionally, the Fed implemented the less restrictive of the two options on network non-exclusivity.

Federal Reserve Final Proposal

The Fed released a final Durbin “regulated” rate of \$0.21 per transaction, plus 0.05% of the transaction value, with the possibility of an additional \$0.01 if banks comply with fraud prevention procedures. An average transaction of \$38 would garner an interchange fee of \$0.24, a significant reduction from the average \$0.34 paid by a typical supermarket retailer today but double the amount food retailers were anticipating to pay. The new rates go into effect on October 1st, 2011.

Regarding network non-exclusivity, the Fed chose to require two non-related networks. A card issuer has to provide two pin, two signature or one pin and one signature networks that are not related on each card. For example, an issuer cannot choose MasterCard (signature) and Maestro (pin) as MasterCard owns Maestro. The Fed chose the less restrictive option of two options presented in the proposal, released in December 2010. Many observers believed the Fed would break open the exclusivity agreements between issuers and networks by requiring four total unaffiliated networks (two pin and two signatures).

Continued on Page 2...

Inside this issue:

The Durbin Amendment/Federal Reserve Update	1, 2
Self-Service Technology – Changing the way we shop	3
PCI Update	4, 5
What is Cloud Computing?	5, 6

Durbin Amendment-Continued

Timeline

July 2010	Bill passed; Retailers could impose a minimum for credit card transactions up to \$10, effective immediately. Additionally, Retailers can begin to provide cash, check and debit card discounts to consumers.
Dec 2010	Federal Reserve releases proposal regulatory draft on debit card fees that are reasonable and proportional to the actual cost. The Fed also requested public comment on the draft.
Feb 2011	Deadline for public comment.
Mar 2011	Bills are presented in the US House and Senate requesting a delay of the Durbin Amendment for one and two years, respectively. Federal Reserve Chairman, Ben Bernanke informs the Senate that providing a final draft on regulation by the April deadline would be unlikely, but the Federal Reserve is still committed to reach the July 2011 deadline when the regulations go into effect.
June 2011	Tester's bill to delay Durbin's implementation falls short of the 60 votes needed to avoid a filibuster after gaining a majority vote in the Senate. Federal Reserve releases final regulations on the Durbin Amendment.
July 2011	Original date for the Durbin Amendment regulations to go into effect.
Oct 2011	Durbin Amendment regulations go into effect.

Redefining Debit

Durbin expands the definition of a debit transaction to include signature debit (for transactions subject to regulation), in addition to pin debit transactions. Signature debit transactions historically receive credit interchange, but after October 1st these transactions will be subject to the regulated debit rate.

Example Rates for a \$35 transaction:

<u>Transaction Description</u>	<u>Trans Rate</u>	
	<u>Prior to Durbin</u>	<u>Post-Durbin</u>
Signature Debit ¹	\$0.35	\$0.33
Signature Debit ¹ "Regulated"	\$0.35	\$0.24
Pin Debit ²	\$0.35	\$0.35
Pin Debit ² "Regulated"	\$0.35	\$0.24

¹ VISA US Consumer Debit: CPS Supermarket – All Other Rate: October 2011 Price Schedule

² Interlink PIN Debit: Supermarket – Tier IV: October 2011 Price Schedule

Identifying Regulated Transactions

The issuing bank determines a regulated transaction. About 580 banks, in the US, have assets in excess of \$10 Billion and therefore are subject to Durbin. Over 14,000 smaller banks fall under the \$10 Billion asset threshold and are not subject to Durbin regulation.

Identifying regulated transactions is difficult, prior to October 1, 2011, as transaction data by issuer is not readily available. A rule of thumb is 60% of debit transactions (PIN and Signature) will be regulated.

The benefit a retailer will receive from Durbin is largely driven by the market share of large banks in the retailer's community. For instance, in a city without a significant big bank presence a retailer will have significantly lower benefit from Durbin. In contrast, in a city with significant big bank presence a retailer will, most-likely, have a significant impact from Durbin.

Banks Response to Durbin

Banks are demonstrating they will recoup revenue lost to Durbin directly from customers. Reward programs on debit cards have all but been eliminated as banks anticipate Durbin. "Free Checking" is receiving a facelift, too, as accounts require a \$1,500 minimum balance or paycheck direct deposit to avoid monthly maintenance fees. Most recently debit card users are receiving monthly surcharges. Some banks are implementing debit card monthly usage fees.

Self-Service Technology – Changing the way we shop

Mobile Self Service in the Supermarket

Customer self service has been a growing trend in supermarkets for years. Self checkout solutions have provided consumers with the option to scan and bag their own orders at checkout. These systems provide benefits to both the consumer and the retailer. The consumer perceives a speedier checkout process, especially when used for express size orders, while the retailer can utilize a single associate to oversee multiple "lanes". But, they are costly to implement with a basic four lane system approximately \$100,000.

Now a new generation of self service is on the supermarket horizon. This is "Mobile Self Service" and it is accomplished through the use of smart phones by a customer to scan and bag their order as they shop. Mobile Self Service is in the experimental stage within many retail organizations. The goal is to make the shopping experience easier while increasing customer loyalty and reducing retailer costs.

Ahold is piloting a mobile self scan solution from Modiv Media at three Stop & Shops in Massachusetts. The system enables customers who download an iPhone app to scan the bar codes of each item they're buying and bag the items as they continue to shop.

The app is linked to the shopper's customer-rewards card, so that customers can receive targeted specials and coupons related to items they like as they shop.

In addition to self scanning, the mobile app can direct customers to locate products on their shopping lists, helping to alleviate one of the major frustrations food shoppers have.

But, like any new initiative there will be hurdles to overcome before these solutions become mainstream.



As with any self service option, the issue of security and shrink must be addressed. How is a retailer to ensure that all product selected and bagged is paid for? How often do you "audit" a customer's order before there is a level of acceptable trust achieved? How will these audits affect a customer's loyalty to the store?

How to handle random weight items? Self service scales in the various departments or handled at the time of checkout?

Do you direct mobile self service customers to self checkout kiosks used as "payment stations" or to cashiered lanes? How will coupons be processed and gift cards authorized?

These are just some of the questions that will need to be considered and answered during the planning process for any retailer moving towards Mobile Self Service.

Despite some of the successes of self-service in the retail grocery space, the industry and consumers are still weighing their options. Recently, Albertsons LLC and Big Y have removed self-checkout units from their stores. With the ever changing technology and the consumer demands for more options, the self-service solutions of the future will be driven by technology advancements and consumer adoption.



PCI Fact—Small Merchants Are Getting Breached

Hackers Use the Internet to Steal Credit Cards

It is time for everyone to acknowledge a painful yet simple truth – computer hackers are targeting small merchants to steal their credit card data. These breaches are happening at an alarming rate, but only the massive ones such as the recent Sony website attack which brought down their on-line gaming network, or the Michaels' Store breach which affected outlets in at least 20 states garner national media attention. Hitting closer to home, the Hannaford Brothers grocery chain suffered from a serious data breach that might have exposed as many as 4.2 million credit cards. With so many large breaches in the news, small merchants believe, somewhat erroneously, that they can slip away unnoticed by the computer hackers on the Internet who make a living from stealing sensitive data. If you think that you are too small to need to worry about this problem, than you need to understand how the world of computer hacking has changed.

Let's compare a large company to the typical Retail Grocer to see why hackers focus on the little guy:

Factors for a Breach	A Large Merchant Has	A Small Merchant Has
Computer Staff	A budget for full-time computer, network, and security employees to maintain corporate data and integrity.	Small or no full-time staff to handle computer issues of any kind.
Credit Card (PCI) Compliance Efforts	A compliance program in place if it is large enough. The credit card companies demand that large merchants supply them with a fully documented compliance program that has been validated by an approved third party security expert.	Minimal validation requirements which often leads to incomplete security programs. Since no one is forcing the issue, many grocers ignore their responsibilities completely. This invites a hacker to target them.
Monitoring Tools	A sophisticated computer network that often includes a process to monitor unusual activity or unexpected data access. This is usually manned by a staff whose sole job is to recognize and catch illegal entry into their networks. Therefore, hackers who go after large companies know that there is an increased risk of being caught by this team.	No monitoring in place and no one is trained in modern incident response techniques. Hackers do not fear that their efforts will be detected until the damage has already been done, and they are long gone.

The small merchant breach has become so prevalent that it was recently (July 21, 2011) the leading story in the Wall Street Journal® in an article entitled *Hackers Shift Attacks to Small Firms*. Most security experts agree that small businesses will continue to be the focus of these attacks. Data from Verizon Business Services and the U.S. Secret Service indicate that there has been over a 500% increase in the number of small businesses that have been attacked and successfully penetrated which has resulted in the loss of credit cards. To make the matter worse, Retail Grocers tend to have more complicated internal systems than other small retailers such as restaurants, and complexity naturally leads to more opportunities for a hacker to exploit your network.

What Can A Retail Grocer Do To Protect Sensitive Data

The first step in avoiding a problem is knowing what it is. In a nut shell, thieves want access to the credit cards that pass through your systems every time you accept a credit card. Hackers also know that computer security is hard. If you truly want to be secure against this rising threat, then you need to treat your electronic security as if it were equally important as your physical security. Would you leave your safe unlocked with your doors open while the store was unmanned? The answer is of course not, but if you do not properly protect your computers, you are in essence doing just that with your credit card data.

Continued on Page 5...

PCI Fact—Continued...

For most operators who take this problem seriously, they obtain technical assistance from a company that specializes in the Payment Card Industry Data Security Standard, PCI for short. PCI is the minimum set of requirements that the major credit card companies (Visa, MasterCard, American Express, Discover, and JCB) expect merchants to implement to keep credit cards safe. The standard covers 12 primary requirements, each of which has numerous sub requirements attached to them (approximately 284 elements in all). Navigating PCI with a company who understands the intricacies of the standard, not only reduces the work you must accomplish on your own, but it helps protect you and ultimately your customers from the looming threat of computer hackers that are relentlessly trying to steal credit cards from you. Remember, to keep your credit cards safe, your security can never fail. A hacker only has to be successful once to steal your data.

Do you need help protecting your locations against hackers? Contact our Retail Technology Department for more information regarding how to protect your store or chain against cyber criminals and a breach of your data.

What is Cloud Computing?

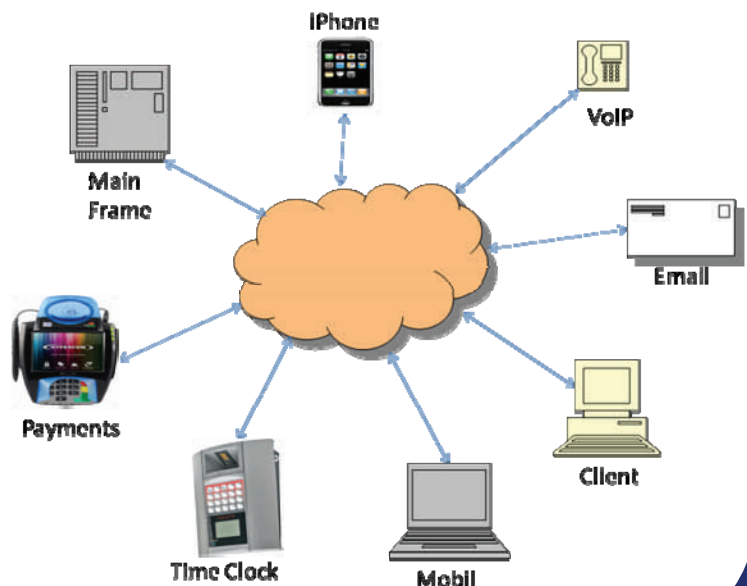
The Internet

What is the Internet, exactly? To some of us, the Internet is where we stay in touch with friends, get the news, shop, and play games. To some others, the Internet can mean their local broadband providers, or the underground wires and fiber-optic cables that carry data back and forth across cities and oceans. The Internet is a fascinating and highly technical system, and yet for most of us today, it's a user-friendly world where we don't even think about the wires and equations involved. The Internet is also the backbone that allows the World Wide Web that we know and love to exist. With an Internet connection, we can access an open, ever-growing universe of interlinked web pages and applications.

Cloud Computing

Modern computing in the age of the Internet is quite a strange, remarkable thing. As you sit hunched over your laptop at work or at home doing your banking, paying bills, email, blogging, watching YouTube videos or using a search engine, you're actually plugging into the collective power of thousands of computers that serve all this information to you from far-away rooms distributed around the world. It's almost like having a massive supercomputer at your beck and call, thanks to the Internet.

This phenomenon is what we typically refer to as **Cloud Computing**. We now read the news, listen to music, shop, watch TV shows and store our files on the web. In the grocery industry we are using cloud computing to solve business needs such as email, Time & Attendance, Payroll, credit/debit card processing, ordering product, and many others cloud services. The end result; we spend less time and money supporting an internal technology infrastructure to support these business processes. The movement of many of our daily tasks to cloud computing enables us to live more fully in the real world.



Cloud Computing—Continued...

Cloud Computing Issues

Cloud Computing is not a silver bullet that solves all our needs, it spans various models and types. Computing on the cloud requires vigilance about security, manageability, standards, governance, and compliance. The same security principles that apply to on-site computing apply to cloud computing security. Personal identity information has to be managed so that access to computer resources, applications, data, and services is controlled properly. Consider the security and privacy of your home: door locks and alarms help protect you from burglars, but curtains and blinds keep your home life private from passersby. In the same way, browser security helps protect you from malware, phishing, and other online attacks, while privacy features help keep your browsing private on your computer.

The Future

The future is unfolding quickly. It has been said that 1 year in computer technology is like 10 years in the automobile industry. In the 1980s, PC computing showed us just how fast new computing technologies can reach the world. Cloud computing will move much faster, because it has several advantages, including today's Internet. In a few years, we will go to our cloud desktop. It will probably look a lot like today's PC desktop. The underlying technologies will be different, but we'll leave those details to the techies. Soon, the hype will subside, but the cloud will be here to stay. We will use it without thinking about it. We'll simply log on to do whatever we do.

Credits:
Cloud Computing for Dummies
20thingsilearned.com

Retail Technology Professional Services Contacts

For additional information regarding any of Unified Grocers' Retail Technology products and services, contact:

Southern California

Tim Eddy
(323) 729-7310
teddy@unifiedgrocers.com

Oregon

Dan Morris
(503) 833-1825
dmorris@unifiedgrocers.com

Northern California

Chris Barcal
(916) 521-9444
cbarcal@unifiedgrocers.com

Washington

Linda Robinson
(206) 764-7614
lrobinson@unifiedgrocers.com