First Data

A First Data White Paper
October 2010

Payments 101: Credit and Debit Card Payments

Key Concepts and Industry Issues

Table of Contents:

Introduction

Credit and debit card acceptance enables merchants to sell goods and services to customers who increasingly choose electronic forms of payment over other payment types.

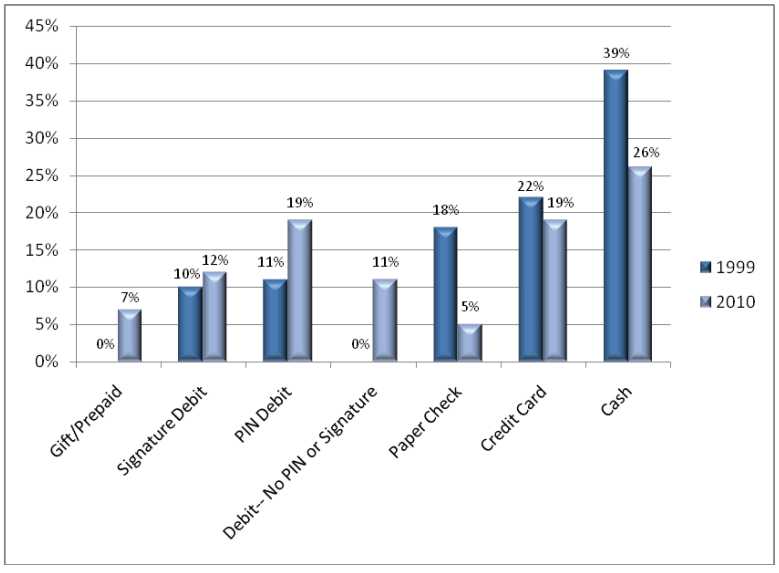
This paper is aimed at merchant executives looking for a basic overview of the credit and debit card markets, including the key trends and issues that they should keep in mind while developing their payments strategy.

Continued Rise of Credit and Debit

Credit and debit cards have increasingly become the preferred methods for consumers to pay for goods and services, making these forms of electronic payments an indispensable way for merchants big and small to conduct business. The trend of rising usage is predicted to continue for some time. Credit and debit card transactions surpassed more than 50% of all non-cash transactions by 2006, up from 42% in 2003, according to a tri-annual study by the Federal Reserve.

Thus, as time passes, it's no surprise cash has lost out to almost every form of electronic payments in stores. Cash transactions, at 10 per month in 2010, represented 26% of a customer's in-store purchases, down from 39% in 1999, according to a 2008 study by Hitachi Consulting and BAI. Credit cards decreased over the time period, from 22% to 19% transactions per month -- while debit cards continued their rise, accounting for 14 transactions per month in 2010, or 42% of all purchases, up from 21% in 1999.

Exhibit 1: In-Store Transaction Mix, 1999 and 2010



Source: Hitachi Consulting and BAI. "2010 Study of Consumer Payment Preferences," September 2010.

On the Internet, it's a similar story of dominance. Credit and debit cards made up 74% of all purchases in 2008 (Internet payment services – mainly PayPal – accounted for another 19%). And it's just the beginning for growth in the category: e-commerce comprised just 3.3% of total retail sales in 2008, up from 2% in 2004.

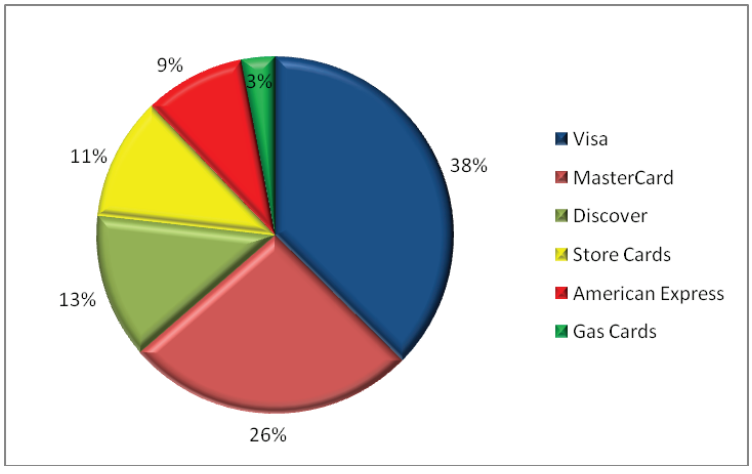
Credit Cards

The concept of a charge card dates back to the 1920s in the United States, when it was used to sell fuel to the nascent market of automobile owners. In 1938, companies started to accept each other's cards. Yet it wasn't until Bank of America Corp. launched "BankAmericard" in 1958 did the modern day concept of the credit card exist. This was the first product of revolving credit that was issued by a third-party bank and accepted by a large number of merchants. Until then, cards tended to be issued by merchants and were accepted by only a handful of other retailers. Later, a group of banks in 1966 issued Master Charge to compete with BankAmericard, the precursor to the Visa® system. MasterCharge evolved into MasterCard®.

Visa and MasterCard were originally owned by groups of banks; they now have been spun off as separate, publicly-traded companies. Risk, from a cardholder perspective, is borne by the banks that use the brands on the cards they issue. In the credit card world, there are also card brands that act as issuers themselves - American Express® and Discover® - and those companies assume the risk of extending credit to their cardholders. However, since a 2004 Supreme Court ruling in Discover's favor upheld a lower court's ruling that Visa and MasterCard could not prevent their issuing banks from also issuing a Discover card, Discover and American Express have moved to create open loop environments where banks can issue their cards.

Credit cards are accepted by most merchant types; historically, they were most frequently used for discretionary and luxury purchases such as travel and entertainment, department stores, and restaurants. They were also commonly used to purchase gasoline. In the 1980s and 1990s, they became a popular option for customers at discount stores, grocery stores and drug stores. Credit cardholders carry an average of four credit cards in their wallet, but use just 2.2 of them in a given month. Visa represents 43% of all general purpose cards carried, while MasterCard holds 36% of the market share. About 54% of cardholders pay their balances in full, versus 46% who carry a balance (these are also known as "revolvers").

Exhibit 2: Network Share of General Purpose Cards



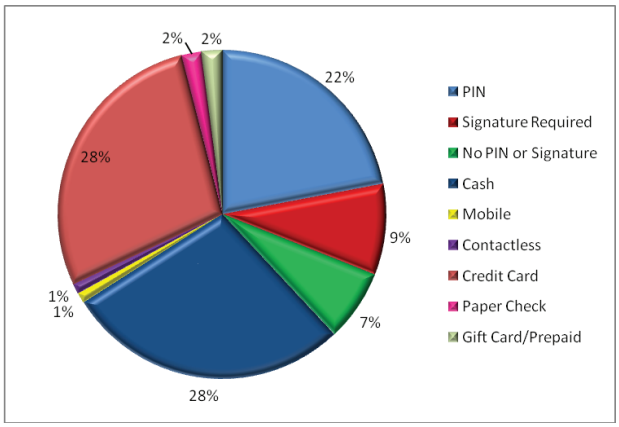
Source: Hitachi Consulting and BAI. "2010 Study of Consumer Payment Preferences," September 20108.

Rewards have also become a popular feature. About 76% of credit cardholders receive rewards on at least one card, with 51% saying the rewards have a strong impact on usage. All told, 58% of all credit cards earn rewards.

Debit Cards

Debit now ranks as consumers' favorite way to pay, with 38% saying they prefer the method for in-store transactions, followed by cash and credit cards at 28%. Debit remains most popular in its traditional venues: grocery stores, drug stores, and discount stores, yet it is also a popular choice at department stores, gas/convenience stores and restaurants.

Exhibit 3: Most Preferred Payment Method



Source: Hitachi Consulting and BAI. "2010 Study of Consumer Payment Preferences," September 2010.

In fact, debit cards have become so popular they have begun to overtake credit in the United States in terms of dollar volume. For example, Visa debit cards generated $1.09 billion in volume in the fourth quarter 2008, compared with $952 million for the network's credit cards, according to a Mercator study. This dovetails with the first year-over-year decline on record of consumer revolving credit, which fell to $931 billion in 2009, down from $963 billion in 2008. Time will tell if this is due to the recent recession or a sign of a more permanent trend.

Signature Debit vs. PIN Debit

Debit cards, which are linked to customers' checking accounts at banks, come in two forms: signature-based and PIN-based. Both capabilities typically reside on the same card. Signature-based debit transactions (also known as "offline debit") tend to be routed through either MasterCard or Visa, much like a credit card transaction. These transactions are debited from a customer's account about two days after the purchase – similar to credit transactions. The process uses two separate messages for authorization, clearing and settlement. Consumers typically do not pay a fee for signature-based transactions, and the logo for the association is on the front of the card.

PIN-based debit (also known as "online debit") requires the consumer to enter a personal identification number – four to 12 digits long – at the point of sale (POS); the transaction is then routed through electronic-funds-transfer (EFT) networks such as STAR®, Pulse®, NYCE®, MAC®, and SHAZAM®. These all require users to enter a PIN for both ATM and POS transactions. PIN transactions also can be run through EFT networks at MasterCard (Maestro®) and Visa (Interlink®). The PIN-based format uses a single message for authorization, clearing and settlement. Unlike signature debit, the customer's checking account is debited immediately, much like an ATM withdrawal. And also similar to an ATM withdrawal, the issuing bank may charge the customer a fee to make a POS purchase.

Yet for merchants, fees for accepting PIN-based debit transactions have historically been lower than those for the signature-based option – the need for a valid PIN combined with the immediate debiting of funds makes them less risky, thereby translating to a lower cost. Signature-based debit cards, on the other hand, come with higher fees to account for their greater risk, in part due to the chance that the user might be forging a signature.

Consumer Preference and Rewards

In terms of branding, most debit cardholders report that their card has a Visa, MasterCard or Discover logo. Yet they prefer PIN debit – which relies on the networks indicated on the back of the card – with 28% of consumers saying they favored the payment method versus 9% listing signature-based and 7% stating no PIN/no-signature as their preference. Cardholders said they prefer PIN-debit because it is more secure, faster and easier to use than signature debit. Those favoring signature debit cite convenience of not having to remember a PIN, the lack of fees, and security as reasons they prefer the method of payment.

Debit rewards programs are growing more popular as usage increases. They are generally offered by signature-based debit cards through Visa and MasterCard, with the fees paid by merchants – enabling issuers to fund the programs. Most debit cardholders (59%) are aware of rewards programs, with 17% saying they received rewards for purchases in 2008, versus 8% five years earlier.

Key Credit and Debit Concepts

There are several areas within the credit and debit card landscape that have a significant impact on merchants. Data security/PCI compliance, interchange, a merchant's POS environment, and the ongoing regulatory focus by Congress on credit and debit cards top the list. Now, transaction routing also enters into consideration as a result of the recently passed "Durbin Amendment," part of the Dodd-Frank Wall Street Reform and Consumer Protection Act—the new financial reform law. The provision requires the Federal Reserve Board to determine how much in interchange fees banks can charge retailers for debit card transactions and it provides merchants the ability to choose which debit network to route a transaction. The following sections discuss the network routing paths in more detail.

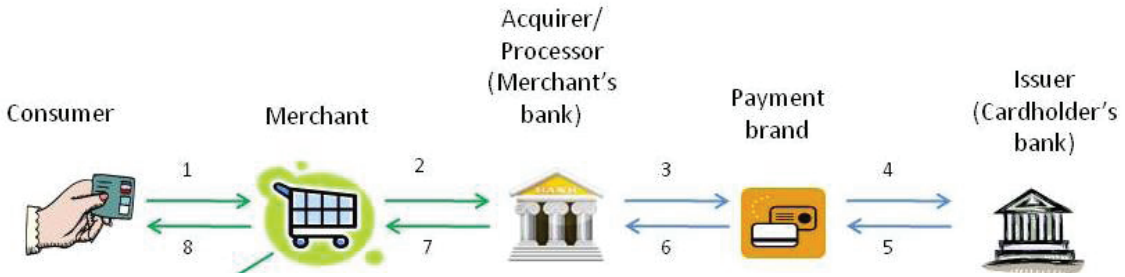
The Path of a Transaction

Signature debit transactions (which occur on the Visa, MasterCard and Discover networks) and credit transactions follow essentially the same processing route. As mentioned previously, the process uses two separate messages for:

1. Authorization
2. Clearing and settlement

Exhibit 4 outlines the authorization process.

Exhibit 4: Authorization - Simplified Transaction Flow for Credit and Signature Debit



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

PIN-based transactions have an additional step if the merchant and issuing banks belong to different EFT networks. If so, the transaction passes through the acquiring processor, then on to a gateway processor that acts on behalf of a national EFT network, such as Visa's Interlink or MasterCard's Maestro. These national networks act as a bridge between the regional ones. With the gateway processor, the transaction is then routed the same way to the issuing bank's processor, then on to the issuing bank for authorization.

For example, say a customer makes a purchase using a PIN-based debit card, which will often be branded with one of the regional EFT networks such as STAR, NYCE or Pulse. After the card is swiped in the POS terminal, the customer enters a PIN and the transaction is routed to the merchant's bank processor. The transaction contains a message including the account number and transaction amount. Assuming the merchant and issuer bank are part of the same network, the acquiring processor then sends the message to the network, which then forwards it to the issuing bank's processor. That processor then sends the message to the issuing bank, which authorizes the transaction and posts it to the cardholder's account. The issuing bank then sends settlement funds to the EFT network. The authorization decision is then sent back via the same route in reverse, all the way back to the POS terminal. These PIN is encrypted and decrypted using secure encryption keys throughout the process.

Interchange

Interchange is a fee:
- → largest component of the discount fee
- → charged to acquiring banks
- → set by the payment brands (Visa, MasterCard, etc.)
- → paid to the issuing banks

The interchange fee is typically composed of two basic parts: a charge representing a percentage of the transaction, and a flat transaction levy. For example, say a customer buys shoes that have a total cost of $100 at a retail store, using a credit card. At a rate of 2% and 10-cent fee, the total interchange would be $2.10. Signature-based debit cards and online PIN-based debit cards are priced this way, but PIN-based counterparts in most cases are less expensive.

The interchange rate charged depends upon a number of factors including the network being used, the card type (i.e., credit vs. debit, rewards card vs. standard card, etc.), how the payment is made (i.e., in-person, over the Internet, via phone, etc.), the industry and size of the merchant, the region or country where the purchase takes place, etc.

Discount Fees

Discount fees are charged to merchants by their merchant acquirers and include the interchange fee, which makes up most of the levy. There are varying methods in which discount fees are negotiated and charged. Discount fees may be bundled, where there is a set rate, including acquirer fees for its processing services, the payment-brand assessments, and network access fees. (additional fees charged by the payment brands to settle a transaction).

Chargebacks

Chargebacks result when an issuer charges back the purchase amount to the merchant. This is generally the result of a customer complaint to the issuer. Chargebacks protect consumers in the event of a fraudulent transaction, customer dispute, or a technical error such as being charged twice for a transaction. Merchants, following card payment brand rules, can dispute a chargeback with the aid of their acquiring bank or processor. Best practices to assist merchants in processing methods to minimize chargeback are available at www.MerchantInsider.com.

Compliance

The payment card industry is rapidly changing, fueled by technological advances in software, systems and hardware. Yet along with this growth has come a surge in technology crimes, leading to stricter and more complex standards for anyone who stores, transmits, or processes payment card data to adhere to. High-profile data losses at merchants, processors and issuers has led to the development of the Payment Cardholder Industry Data Security Standard (PCI DSS), originally created by Visa and MasterCard to protect cardholder information and reduce data theft. The PCI DSS consists of security requirements for any organization that comes in contact with payment card data. The payment brands (Visa, MasterCard, Discover, American Express and JCB®) enforce compliance with the PCI DSS for member banks, merchants, and service providers. Certain significant PCI DSS requirements (and payment brand rules) state that merchants may not store some elements of magnetic-stripe data after an authorization is obtained on a credit card, and account numbers must be protected (or rendered unreadable) anywhere they are stored.

Transaction information that is maintained must be safeguarded according to stringent guidelines. By becoming PCI compliant, merchants protect customers from losing valuable card data and insulate themselves from possible legal action and certain fines from the payment brands.

If a merchant is the source of a breach, then the liability potential increases to include:

- → Losses from fraud as banks and processors can reclaim losses they sustain as a result of the breach
- → Brand damage - resulting from the public reporting of breaches often being required by law.
- → Potential lawsuits from customers, financial institutions, card processors, payment brands, state attorneys general, etc.
- → Government oversight depending on the extent of the breach

Each Spring and Fall, the card associations evaluate their processes and regulations and announce their anticipated changes in a release statement. These changes apply to all credit and debit card processors and may impact the fees and rates you incur to accept electronic payments.

Failing to comply with the PCI DSS can also result in a merchant losing the right to offer credit card payment options and incur non-compliance fines.

Fraud

Credit cards top the list as the underground economy's most popular item of stolen data. The price for a stolen credit card ranges from 10 cents to $25 per card, with discounts offered for bulk purchases. Card fraud can hit the bottom line of merchants hard – in terms of lost/stolen goods or services, chargeback penalties, and related processing and currency conversion fees.

The Internet has allowed cybercriminals to gain momentum and develop an efficient, global marketplace, where it is relatively easy to buy and sell fraudulent goods and services online, hire contractors and exchange useful industry information. This increasingly sophisticated underground marketplace is providing cybercriminals, often organized crime syndicates, a profitable environment for buying and selling millions of dollars' worth of stolen goods and fraud-related services. While it is impossible to anticipate or prevent every attack, one way to stay a step ahead of these criminals is to have a thorough understanding of how they operate their business, both on the frontlines and behind the scenes. Knowing how they attack, how they sell data and where the vulnerabilities are in the system gives those affected by fraud a better chance of mitigating the risks and stopping the criminals in their tracks.

First Data provides businesses with a solution called TransArmor, which is a payment security product embedded into a terminal that removes card data completely from the merchant environment. TransArmor uses a dual layer of security, encryption and tokenization, to protect customers' sensitive information and limit merchant liability in holding customer data. When a customer uses their credit card, the card number is encrypted when the card slides through the terminal and decrypted by the acquiring bank. With this solution, credit card data is not stored at the merchant location. By removing sensitive card data and replacing it with a card-based token number, it shifts the burden of storing and protecting card data from the merchant to the payment processor.

Terminals and Point of Sale (POS) Hardware and Software

Terminals

Businesses require terminals to process electronic payments at the POS. A terminal is a mechanism for merchants to be able to accept electronic payments—a device that will capture and transmit card information for processing via card payment brands. There are many standalone terminal providers, including Verifone, Hypercom, and Ingenico. First Data also offers its own line of terminals—the FD Terminal series. Merchants typically look for a terminal that can process all types of transactions from a single source—including credit cards, debit cards, Electronic Benefits Transfer (EBT), gift cards, loyalty cards and checks. Merchants want to find a reliable terminal with ultra-fast processors and communications hardware to make sure transactions are handled quickly and accurately. And they want a terminal that is easy to use with a built-in printer and intuitive touch-screen interface. For merchants who travel or seek to receive payments remotely, there are terminals enabled with wireless technology so they can process transactions no matter where their business takes them.

An important thing to look for in a terminal provider is service and support—merchants want someone who can help them configure their terminal and quickly manage any issues that might arise. Look for a provider who offers overnight replacement terminals when there's a technical problem, and a customer service team to call to answer any questions.

While small merchants often rely upon terminals to process transactions from beginning to end, larger merchants typically operate POS systems that integrate hardware and software—they use third party POS software that has the ability to send cardholder data to a processor using software embedded in the register. They might have a PC-based solution with an attached peripheral to handle credit and debit card processing. Both solutions require a provider that enables fast, accurate and reliable transaction processing.

Peripherals

Peripherals are add-on devices that provide a merchant with additional transaction functionality at the POS. For example, a merchant with a cash register might want to integrate a PIN pad that allows for debit transactions. The addition of a PIN pad would allow consumers to swipe their card and enter their PIN number at the point-of-sale. Other types of peripherals include contactless readers, for merchants that want to offer 'tap and go' functionality. The peripherals are typically compact and are a complement to the existing merchant transaction capabilities.

Point-of-Sale Software

Increasingly merchants are opting for payment functionality that is embedded within the POS system. This model requires the POS manufacturer's software developers to code to a provider's specifications. Merchant benefits include consolidated reporting across payment types, decreased cashier error (no manual keying of transaction amount into a standalone terminal), and single source provider of the POS system and payment interface. Examples include the IBM ACE Supermarket system, MICROS restaurant POS system, and Radiant's Epsilon petroleum solution.

Connectivity Options

Merchants can choose from a variety of connectivity options to align with their business needs, including securely accepting all types of credit cards, debit cards, checks and gift cards. Cost, speed and customer convenience are the key factors that drive decisions about which connectivity options make the most sense for a particular merchant.

1. Dial-up: Dial up service uses your existing phone line. When you are ready to begin a transaction, the terminal uses the phone line to open a call to the processor. It is generally a slower transmission of data, but since every business has a phone line, it is readily available and a low cost solution. If you have multiple terminals at the merchant locations, you will need one telephone line per terminal.
2. Wireless: This terminal doesn't require a phone landline—you can take the terminal wherever your sales occur. It requires cellular service to transmit a transaction from the "remote" location. The terminal is all encompassing—it typically has a printer and Payment Card Industry PIN Entry Device (PCI PED). This type of terminal is ideal for service industries like delivery services, home services, etc.
3. IP and VPN: This is a low cost solution that takes advantage of your existing IP network infrastructure. It also offers a low cost, high-speed solution for merchants with an established Internet based infrastructure. Up-time depends on your service provider.
4. Wi-Fi: The Wi-Fi solution takes advantage of your existing IP infrastructure, so there are no phone lines required. It offers a low cost, high speed solution for a merchant with an established wireless network. It is a bit more complex to maintain and operation is reliant upon an IP services provider—but if you have a good wireless infrastructure, it is an ideal option.
5. Dedicated or Leased Lines (aka 'Frame Relay'): This solution provides faster throughput over a regular IP connection. However, it is the most costly option due to the required changes and upgrade to the infrastructure, and requires dedicated technical resources, such as staff and additional hardware. This is commonly used for large, national merchants with high-volume, multi-lane environments.

Strategic Importance of Payments

Developing a payments strategy can help merchants better plan for the future, keep pace with their competitors, and maximize their financial performance. Below are additional considerations for merchants that are developing and implementing their payments strategy.

Benefits for Merchants and Consumers

Along with the easier-to-measure costs associated with accepting electronic payments, credit and debit offer a number of benefits to merchants. Advantages include:

1. Greater revenues: according to industry research, average transaction amounts tend to be higher when using electronic payments.
2. Improved security over cash, since cards reduce the amount of on-site cash and related cash theft.
3. Reduced costs associated with handling cash.
4. Improved reporting compared with cash, with some acquirers offering online access to information such as recent transactions, adjustments and bank deposits for a range of time periods (i.e., daily, weekly, monthly, etc.). Strong reporting provides merchants with increased visibility into their business, which can aid in planning.

Consumers are turning more to credit and debit cards mainly due to convenience. Customer comfort levels and perceptions of speed for credit and debit cards are similar to cash. Consumers also benefit by receiving fraud protection for credit and debit cards, such as an out-of-pocket limit of $50 in the event of theft of the card. For credit cards, buyers can take advantage of getting access to a line of credit on demand. Meanwhile, debit cards offer consumers quick access to their checking accounts without having to write a check. And many consumers prefer to use debit rather than credit to better manage their spending and not add to a revolving balance.

Understanding the Payments Mix

Merchants can take steps to lower their payments-related costs while maintaining or increasing their revenues. Directing customers to a particular payment type seems to be the preferred method among some merchants. For example, steering customers to lower cost PIN debit generally saves merchants money (compared with signature debit), while still offering customers the convenience of debit payments.

Merchants can implement different approaches to encourage customers to pay with a particular payment type:

1. Rewards programs. Coffee houses and fuel merchants have been the most aggressive in guiding their customers to use gift cards and certain types of debit card products through targeted rewards. Rewards programs can serve the dual purpose of lowering payments costs and increasing revenues, although, at least some of the cost savings are applied to maintenance of the rewards program.
2. Consumers have choices at the POS. Some merchants take steps to guide customers to PIN debit by first presenting customers with a PIN option; to conduct a signature-based transaction, the user must cancel the screen then search for the option on a subsequent screen.
3. The Durbin provision of the Wall Street Reform Act allows merchants to set a minimum amount for credit card acceptance, and to establish discounts or incentives to entice customers to pay with an alternative method.

What to Look For in a Provider

Knowing what to look for in a provider of credit and debit card acceptance products and services can help merchants stand apart from their competitors, maximize revenues, and minimize troublesome issues.

Security

Now more than ever, merchants need to make sure providers are aware of the latest security trends. A provider should work closely with merchants and financial institutions to help address risk and fraud across the entire customer life cycle with a comprehensive set of prevention and detection solutions. It should offer customized, innovative solutions that enable merchants to stay ahead of trends to effectively manage risk and to detect, prevent and reduce fraud. That includes tools that help prevent credit and debit card fraud, facilitate PCI compliance and offer transaction data protection solutions. Merchants should also work with a provider that helps ensure compliance with all industry encryption standards for the transmission of data. The vendor should also be knowledgeable about standards such as the PCI DSS and Payment Application Data Security Standard (PA DSS). And the provider should be able to work easily with third parties to provide the tools necessary to support merchant compliance.

Reliability

Whether a cardholder is purchasing a gift on the busiest shopping day of the year or buying tickets to a play right before the opening act, providers need to get it right the first time. Vendors should have multiple flexible processing platforms and full data-center redundancy for maximum uptime reliability.

Relevant Expertise and Expert Advice

A provider should have dedicated account relationship management teams with specialized expertise, so that they can best serve the merchant type and the issues it faces. The provider should proactively work with clients to identify issues as they arise and develop an action plan for resolution. It should also analyze a client's business for potential savings and growth opportunities. The vendor should have a staff with deep knowledge of historical and future payments trends. The provider should also always follow through and often exceed a merchant's expectation across the gamut of issues, including escalations, funding questions, chargeback inquiries, transaction/batch questions and the like. In addition, they should provide a timely explanation of compliance mandates and be their merchants' advocate within the industry.

Portfolio Solutions that Meet Business Needs

A provider should offer competitive rates, transaction security, flexible billing and timely, accurate reporting options. A vendor should have a full range of POS terminals, peripherals and supplies designed to save both time and money while supporting all Payment Card Industry (PCI) compliance standards. The vendor should have flexible payment acceptance options, including credit, debit, check, gift card, Electronic Benefits Transfer (EBT), as well as WEX and Voyager for petroleum clients. The provider should have relationships with all major credit card and debit card companies, including Visa, MasterCard, American Express, Discover, Diners Club®, JCB and STAR. Merchants should have full access to their account information through robust, web-based reporting tools and solutions to help them simplify back-office processes and expedite response time.

Innovation that Helps Grow Business

Significant changes at the point of sale over the last 30 years have been driven by the need to increase the speed and accuracy of transactions for retailers and their customers. Today, the latest developments in POS technology have the potential to make an even bigger impact by moving the point of sale to wherever the customer is. That may mean allowing customers to pay for a parking meter with a mobile phone or checking into a hotel room without having to stop by the front desk. Technology such as portable POS hardware and commerce-enabled mobile devices can provide a more efficient checkout experience by reducing custom ers' overall shopping time. They can also allow retailers to merge sales, marketing and relationship building with the checkout process.

Glossary of Terms

ACH – short for "automated clearing house", a nationwide electronic network for financial transactions. The network clears credit and debit transactions. Rules and regulations for the network are set by NACHA and the Federal Reserve.

acquirer – see merchant acquirer

associations – also referred to as "payment brands" or "network." In the world of credit and debit cards, this is a legacy term that referred to ownership of networks by groups of financial institutions. Today, the word is sometimes used to refer to companies such as MasterCard, Visa, American Express, Discover, STAR, NYCE and others which regulate card acceptance rules and interchange for their member financial institutions.

authorization – the process by which an association or network requests approval with the issuing bank on behalf of the merchant. Once a transaction is authorized, the association sends the approval to the merchant acquirer, who passes it along to the merchant. Then the customer can complete the purchase.

chargebacks – the refusal or reversal by the issuing bank of a transaction presented by the merchant acquirer. Chargebacks result when an issuer returns or ìcharges backî the purchase amount to the merchant.

check – a piece of paper that orders a bank to pay money on the accountholder's behalf. Checks have been losing ground to all other forms of electronic payment, including credit and debit cards, and bill-pay.

clearing – process by which the merchant acquirer sends purchase information to the association or network, which in turn sends it along to the issuing bank. The issuer then prepares the information for the customer's statement.

closed-loop prepaid cards – also known as private-label prepaid cards or merchant-branded prepaid cards, these are offered by a merchant and can only be redeemed in the retailer's stores.

compliance – with respect to credit and debit cards, it refers to all the rules and regulations merchants must meet in order to have the right to accept electronic payments, adhering to formats such as the Payment Cardholder Industry Data Security Standard (PCI DSS).

credit card – a plastic card issued to customers as a way to pay for goods and services, based on a promise to pay for them at a later date.

demand deposit account – a checking account that holds a customer's deposits at a financial institution. Also known as "DDA."

debit card – a plastic card linked to customers' checking accounts that allows them to pay for goods and services. Acting like an electronic check, funds are drawn against the account. Also known as a "check card."

discount fees – fees charged to merchants by their merchant acquirers. The fees include interchange, which is the largest component, along with levies by the acquirer for its processing services. The discount fee may also include assessment fees that are paid to the associations.

EBT – short for "electronic benefits transfer". This is a nationwide system that provides a way for state governments to disburse financial and other benefits via a plastic debit card. Generally, the benefits break down into food and cash.

EFT network – short for "electronic-funds-transfer" network, a telecommunications and payments infrastructure that connects consumers, ATMs, merchants and banks. There are two types of transactions: those at ATMs and those from signature-debit cards at POS terminals.

fraud – with respect to credit and debit cards, the act of illegally taking or falsifying customer accounts in order to steal goods and services.

funding – the process of the acquirer paying the merchant, which happens after the acquirer receives payment from the issuer via the associations.

ISO – short for "independent sales organization." These companies sell services of a bank or processor. They sell merchants both front-end (terminals) and back-end (processing) solutions.

interchange – a fee charged to acquiring banks, set by the associations, and paid to issuing banks for the service of accepting a credit or debit card as payment. Acquiring banks may pass the costs along to merchants via the discount fee.

issuer – a term used to define who issues the credit or debit card. The issuer bears the risk, essentially vouching for the creditworthiness of the customer.

magnetic stripe – a short strip of magnetic tape on the back of a credit or debit card; it holds data that will tell a POS terminal who the cardholder is along with the account number and other secure information not disclosed to the acquirer.

merchant acquirer – either a bank, a processor or independent sales organization (ISO) handling the merchant's card acceptance. A processor or ISO will work with an acquiring bank, which is needed to officially accept payment on behalf of the merchant.

NACHA – an organization that sets rules and regulations – along with the Federal Reserve – governing the ACH network. Formerly known as the National Automated Clearing House Association.

open-loop prepaid cards – also know as network-branded prepaid cards, they can be accepted anywhere the network's cards are taken.

payment brands – also referred to as 'associations'. In the world of credit and debit cards, this is a legacy term that referred to ownership of networks by groups of financial institutions. Today, the word is sometimes used to refer to companies such as MasterCard, Visa, American Express, Discover, STAR, NYCE and others which regulate card acceptance rules and interchange for their member financial institutions.

processor – a company that handles all or some of the functions of a credit or debit transaction, ranging from providing terminals to managing back-end settlement.

PCI DSS – short for "Payment Cardholder Industry Data Security Standard," which was created by Visa, MasterCard, American Express Discover and JCB to protect cardholder information and reduce data theft. PCI DSS establishes and enforces security requirements for members, businesses and service providers. Certain significant PCI DSS requirements state that merchants may not store magnetic-stripe data after an authorization is obtained on a credit card, and account numbers must be protected anywhere they are stored.

PIN – short for the "personal identification number" customers must enter when using a debit card routed through the EFT networks or Visa and MasterCard's online EFT networks. It is the same number used for making an ATM withdrawal.

PIN-based debit – a process where debit transactions are routed through EFT networks, requiring a PIN. Electronic authorization of every transaction and the debits to a customer's checking account are reflected immediately. Also known as "online debit."

POS – point of sale. The site where a customer makes payment via credit or debit cards. Generally terminals are at the cash register, but mobile terminals at restaurants, theme parks, computer stores and other merchants are changing where transactions can be conducted.

prepaid cards – these act much like debit cards: value associated with the card is stored in the customer's account with the issuer. A merchant can offer customers their own "closed-loop" cards, which can only be redeemed at its own stores; general-purpose or "open-loop" cards are issued by banks and can be redeemed anywhere network branded credit cards are accepted. These cards may be reloadable.

settlement – process by which the issuing bank sends payment to the association, which in turn sends it to the merchant acquirer. The acquirer then funds the merchant account.

signature-based debit – a process where debit transactions are routed through the major card associations MasterCard and Visa, much like that of a credit card, requiring the signature of the customer depending on the sales amount. Transactions require two to three days to be reflected on customer account balances. Also known as "offline debit."

Federal Reserve, "The 2007 Federal Reserve Payments Study."
Hitachi Consulting and BAI. "2010 Study of Consumer Payment Preferences," September 2010, pp. 21, 71.
Ibid, pp. 93, 99.
Ibid, p. 35.
Ibid, p. 36.
Hitachi Consulting and BAI. "2010 Study of Consumer Payment Preferences. "September 2010. pp.68
Ibid, p. 24
Mercator Advisory Group, "The U.S. Merchant Acquiring Market." August 2009, p. 16.
McKinsey & Co., "U.S. Payment Trends 2008-2013," January 2009, p. 9.
Hitachi/BAI, p. 68.
Ibid, p. 41.
Ibid, p. 42.

