BUILDING A SYSTEM FOR CARDHOLDERS' TRANSACTION SECURITY

Jose Gonzalez
Conrad Shayo
Frank Lin
Jake Zhu

California State University, San Bernardino
5500 University Parkway, San Bernardino, CA 92407

ABSTRACT
This paper seeks to discuss and develop a solution to a problem that costs billions of dollars every year in fraudulent related losses arising from the use of payment cards such as debit cards, credit cards, charge cards or prepaid cards. We analyze the industry of payment cards, the emergence of the problem, and build a prototype system called QueuePay that allows cardholders to control payments. The main feature for QueuePay is the formation of systematic queues that are authorized by the cardholder. Soon, a website: QueuePay.com will provide services to its cardholders that will significantly reduce the risk of fraud.

INTRODUCTION

Background

Payment cards allow consumers to conveniently purchase goods from physical brick and mortar or online retailers. Rather than carrying large amounts of cash, consumers have immediate access to their bank account funds or credit lines through the use of their cards. The global volume of non-cash payments transaction (using direct debits, credit transfers, cards and checks) has been steadily growing worldwide. In 2010 more than one in three non-cash payments globally was made using a debit card, up 15.2% while check usage continued to decline worldwide (Alidina, Austin, & Barber, 2009-2012).

Aside from not having to carry large amounts of cash in your pocket, using payment cards as a method of payment also allows cardholders to leave a record of transactions. These transactions are available through a monthly bank account or credit card statement which allows people to review their transactions every month in paper form or by logging into their bank's website periodically or even on a daily basis.

One problem though is that, we don't always have total control of what comes out of our accounts. Occasionally, we set up recurring charges or auto debits in one month and forget about them the next month. If we encounter a financial setback we may need to temporarily stop the auto debits from our bank accounts. Some companies require many days of advance notice to cancel an auto debit for a given month. If it's too late for a company to stop an auto debit at the time requested by a cardholder; one solution is to withdraw all of the money from the bank account and immediately closing it in order to avoid NSF charges. Although auto debits and

recurring charges are a good convenience, it is not as convenient when a cardholder needs to stop such debits for any reason.

Moreover, there are many services that require recurring monthly fees such as gym fees, credit monitoring fees, magazine fees or any other monthly fees may create a hassle to the customer since the customer is required to initiate the cancelation process to avoid a recurring charge or auto renewal. This may involve long calls and delays to be transferred to the cancelation department or jumping through other hoops to finally cancel the service. There are many free trial periods of a service that require a customer to issue a payment card number. Many decide they don't like the service but forget to call and cancel and consequently get dinged with a charge. There are times that you may need to listen to many prerecorded marketing messages offering additional products or complete a survey before you may cancel.

The QueuePay solution eliminates the need to withdraw funds from your account or even close an account to stop auto debits. QueuePay will also prevent auto debits to be taken out of your account in amounts that exceed the expected monthly charge. With the ubiquity of payment card use, QueuePay.com is a company that will set the benchmark in a new era of payment cards processing.

An additional problem is that, there is rampant fraud in the payment card industry. In 2010, there was $7.6 billion dollars in payment card fraud worldwide. 47% of that was in the U.S. alone (Robertson, 2011). Fraud situations include: lost or stolen credit cards, fictitious websites, payment card number generators, compromised card number information, and fictitious ATM's.

Cardholders are trying to find methods to reduce the likelihood of being victims of fraud. In many cases, cardholders don't mind taking extra steps to complete a transaction if it means that they will be less prone to fraud. Consumers familiar with PayPal know that an extra step is required to complete an online transaction. The extra step requires the consumer to log in to their PayPal account using their email address as verification that the legitimate consumer is authorizing a payment. This step has proven very successful. However, there are a couple of major setbacks with the current PayPal's business model:

- PayPal's main source of business comes from eBay users.
- Even though thousands of other merchants now accept PayPal as a payment method, many consumers still find themselves having to provide their payment card information to the other millions of merchants who don't accept PayPal.

QueuePay's business model provides a higher level of security without the major setbacks observed with PayPal's model. QueuePay will issue actual payment card numbers to its members to eliminate merchant participation limitations. As an issuer, QueuePay will become a member of the Visa card association and issue payment cards with the Visa logo. In other words, any merchant that accepts a Visa card will indirectly be accepting QueuePay as a mode of payment. Note that only thousands of merchants accept PayPal but there are millions of merchants worldwide who accept Visa but don't accept PayPal.

How the QueuePay System Works

Figure 1 shows how the QueuePay System works. The figure lists five transactions.

- The first transaction represents a deposit of $500. There are two columns in the far right that show the account's virtual and actual balances.
    - The actual balance represents (just like the word implies) the account's actual balance reflecting all deposits and withdrawals that have been authorized and processed.

- Deposits always update the virtual and actual balance in the same amount. No queues are necessary for deposits.

- The second transaction of $102.61 represents a transaction that was originally queued and has already been collected by the merchant.
  - Virtual and actual balance was reduced by $102.61.
  - A memo column gives the user the option to track what was purchased. This field may be left blank or hidden depending on the customer's preference.

Figure 1. Illustration of How the QueuePay System Works

Date	Amount	Description	Status	Memo	Virtual Balance	Actual Balance
03/10/12	**500.00**	Deposit			500.00	500.00
03/11/12	102.61	Amazon.com	Authorized	Books	397.39	397.39
03/15/12	35.63	Walmart.com	Queued	Ink	361.76	-
03/15/12	<20.01	Auth. under $20	Queued	-	341.76	-
03/15/12	45.00	Auth. Under $50	Authorized	Chevron	296.76	352.39

- The third transaction of $35.63 represents an amount that has been placed on queue but not yet collected by the merchant. An example of how this occurs starts with:
  - A customer visiting Walmart.com to purchase ink
  - The customer finds the ink they need and place the item in their online cart.
  - The customer is ready to check out and proceeds to the checkout screen.
  - The customer opens a new tab in their browser, logs in to QueuePay and places a $35.63 transaction on queue.
  - The virtual balance is updated but the actual balance is not.
  - The actual balance will be updated once the transaction is actually processed (just like previous transaction).
  - The description field is also optional; however, if the description is left blank the field will be updated with the merchant's information once the transaction is processed.
- The fourth transaction represents a "less than" queue. An example of this would be a customer that knows they will spend less than $20 at a convenience store.
  - The customer places a queue that will allow him/her to charge any amount from $0.01 to $20.00.
  - The virtual balance is reduced by $20.00. Actual balance stays the same
  - Once the transaction is authorized, the actual amount will appear in the "amount" column. At this point the actual balance will also be updated.
- The final transaction represents the scenario where a "less than" transaction was queued and has already been authorized. An example of this would be a customer who arrived at the gas station and knew that he can fit about $50 worth of gas into his car.
  - The customer placed a "less than" $50 queue.
  - The gas tank actually filled up at $45.
  - The transaction is authorized because the amount is less than $50.

The virtual and actual balance reflects a transaction amount of $45. Placing transactions on queue as a prerequisite for funds to be removed from a cardholder's account significantly reduces the likelihood that unauthorized charges will go through. In theory, the only way an unauthorized transaction will be processed is if the user shares their log in information with someone else. For added security, QueuePay will be using the https:// protocols. This will provide encryption for communication between QueuePay's servers and the associated web servers communicating with it.

Giving cardholders the power to control how and when their funds are released to merchants saves them many hassles. With QueuePay all a customer needs to do is not place the recurring charge in their queue and the service will be cancelled automatically due to nonpayment. QueuePay will offer a feature that will help customers manage their auto debits and recurring charges much easier. The figure below shows the information that a cardholder will be able to see when logging into their QueuePay account under "Recurring Charge and Auto Debit Management" (see Figure 2).

Figure 2. Recurring Charge and Auto Debit Management

Recurring Charge and Auto Debit Management

Frequency	Company	Criteria		Date Range	Contains	Enabled
Monthly	Gas Company	Not to exceed	$85	10th - 15th	"Gas Co"	☑
Every two Months	Trash Company	Not to exceed	$80	1st - 5th	"Trash Co"	☑
Every year	Costco Dues	Exact Match	$115	N/A	"Costco Mem"	☑

Enrolling as a QueuePay Member

The process to begin using QueuePay requires a customer to set up an account online at QueuePay.com. The customer would then be instructed to link their bank account to their QueuePay account. Once funds have been added to the customer's QueuePay account using methods such as ACH or wire transfers, the customer will receive a payment card number via a secure communication as well as an actual card in the mail. Other methods will be available to fund a customer's QueuePay account if the customer does not have a bank account. Such methods may include but are not limited to purchasing prepaid QueuePay debit cards at convenience stores, recharging their cards where QueuePay cards are sold, or enrolling their payroll in direct deposit with a QueuePay issued routing and account number. The concept is simple: A customer places a transaction on queue before the transaction is presented for authorization. If the transaction matches the queue, the transaction will be authorized.

The notification system QueuePay will enable its users to know in real-time their available balance. If they are using their cell phone to queue a transaction amount through text messaging, they will receive a confirmation letting them know if the queue was successfully placed; their available virtual balance, as well as their actual balance (see Figure 1: Illustration of the Transaction in Queue). On the other hand, smart phone apps and web browsers will provide this information once they log into their accounts. Additional notifications will be sent (through user defined preferences) by text or email if an unauthorized transaction is attempted.

Let's say a cardholder's card information is compromised or their card was lost or stolen without the cardholder knowing. If someone tries to use this card, the legitimate cardholder will receive a notification of any failed attempts to charge transactions on that card. Once the QueuePay customer is notified of such attempts, the customer can request for a new card to be mailed to

them. It is important to note that no unauthorized charges will be placed on a customer's account without a preexisting queue authorizing the charges.

BRIEF PAYMENT CARD HISTORY

In the beginning of trading, there was barter, cash and then checks. In the late 1800s, before the introduction of plastic payment cards in the 1900s, merchants and customers used credit coins and charge plates as currency (Woolsey, 2012). In 1946, the Flatbush National Bank of Brooklyn issued the first bank payment card. The card, named 'Charger-It', was invented by Jon Biggins, an employee of the bank, for use between bank customers and merchants (Hardekopf, 2010). Following this invention, Frank McNamara, President of the Hamilton Credit Corporation introduced the then widely used 'Diner's Club Charge Card' for use between subscribers and restaurant owners. McNamara charged cardholders a $3 annual fee and 7% per restaurant transaction. In 1958, American Express introduced a charge card for leisure expenses and in 1966, Bank of America introduced BankAmericard (later became VISA), the first general purpose card that was used across state lines. In the same year, a group of California Banks and Marine Midland Bank of New York (now HSBC Bank USA) formed the InterBank Card Association which created the 'Master Charge: The Interbank Card', now known as MasterCard. By 1970, 16% of all households in the USA were using a bank-type card with 37% of the households carrying an average balance of $839 (Hardekopf, 2010). Today, more than 70 percent of U.S. families own a minimum of one general-purpose payment card (Alidina, Austin, & Barber, 2009-2012)

PAYMENT CARD FRAUD

With the popularity of payment cards, along came a rise in fraud. Criminals are always looking for new ways to gain from the loss of others. For example, between 2001 and 2009, an average amount of US $ 3.1 billion were fraudulently stolen globally (Alidina, Austin, & Barber, 2009-2012). There are two main types of payment card frauds. One involves counterfeiting payment card information, which is usually carried out by organized criminal groups. This type of fraud has a huge effect and it usually affects tens and even hundreds of customers of a bank at a time. The second type of fraud occurs when a payment card is lost or stolen. This type of fraud only affects one or a few cards at a time (Ekrem & Ozcelik, 2011).

Global payment card losses in 2010 totaled $7.6 billion. This represents an increase from 2009 of 10.2 percent. About forty-seven percent ($3.56 billion) of this figure comes from the U.S. (The Nielson Report, 2008). Organized crime committing payment card fraud is a worldwide phenomenon. One well known case is the TJX heist where hackers accessed the merchant's database and stole about 45 million card numbers (Privacy Commissioner, 2007).

There are many different schemes criminal use to commit payment card fraud. Below are a few examples of the many techniques out there. Traditional techniques fetch far less money when compared to modern techniques. Traditional fraud techniques include:

- Application Fraud**:** is where an individual will falsify an application to acquire a credit card. Application fraud can be split into:
    - Assumed identity**:** is where an individual pretends to be someone else.
    - Financial fraud**:** is where an individual gives false information about his or her financial status to acquire credit.
- Intercept Fraud**:** is where a card is applied for legitimately, but is stolen from the post service before it reaches its final destination.
- Lost and Stolen Cards**:** illegal use of lost or stolen cards.

Modern fraud techniques include:

- Skimming**:** where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip is copied from one card to another.
- Site Cloning**:** where a legitimate site is cloned but runs at a different IP address. Sometimes victims receive phishing emails from what appears to be legitimate banks with links redirecting them to the cloned sites asking them to reenter their credit card information. These sites will look very similar to the original site but are actually clone sites.
- False Merchant Sites: such sites are designed to get people to hand over their credit card details without realizing they have been scammed.
- Credit Card Generators: computer emulation software that creates valid credit card numbers and expiration dates. These generators are highly reliable at creating valid credit card details and are available for free download off the Internet (Sylvester, 2012).

The growth of payment card fraud is due to the use of modern techniques. Fraudsters attack merchants' databases and processor data centers to gain access to an abundance of accounts. This results into far more stolen card information than through traditional means such as stealing physical cards from wallets or mailboxes (Alidina, Austin, & Barber, 2009-2012).

CURRENT FRAUD PREVENTION TECHNIQUES USED BY PAYMENT CARD ISSUERS/ACQUIRERS/MERCHANTS

Payment card issuers do their best to keep up with the criminals. For example, a criminal using an assumed identity technique may gather documents and information about a victim in order to call their credit card company requesting a change of address (one controlled by the criminal). After changing the victim's address, the criminal proceeds to impersonate the victim by submitting "proof" of identity to the credit card company and requesting that a replacement card be sent to the new address. Techniques that a fraud detection tool may use would be to look at the address change request and compare it to the person's credit report file. For additional confirmation, a text message and/or automated phone call advising changes on the account is made to all pre-existing phone numbers on file before the change. Additionally, a letter can be sent to pre-existing addresses too. This ensures that if a customer's identity is impersonated, they can be notified right away. There is a whole range of existing tools that help prevent and detect credit card fraud.

Statistical techniques involve data preprocessing techniques for detection, validation, error correction, and filling up of missing or incorrect data. It also involves calculation of various statistical parameters such as averages, performance metrics, probability distributions, and others. Additionally, matching algorithms are also used to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. On the other hand, techniques are also needed to eliminate false alarms, estimate risks, and predict future of current transactions or users.

Artificial intelligence and neural network techniques comprise of the collaborative use of many detection tools that enable unsupervised decisions by the system. For example, sometimes a customer may receive an automated call from their bank after making a large purchase. The automated call would then request verification that this transaction was authorized by the cardholder. Another set of detection tools used in artificial intelligence are expert systems which are used to encode expertise for detecting fraud in the form of rules.

One additional detection technique used is data mining where data is classified, clustered, and segmented in order to automatically find associations in the data that may signify unusual patterns, including those related to fraud. Moreover, machine learning techniques are also used to automatically identify characteristics of fraud. (Sachdeva, 2011).

There are companies that offer tools that integrate many of the techniques discussed in the preceding section. One of the companies is SmartSoft. This company has a line of products that collaboratively uses the tools discussed above. Two of the products offered by SmartSoft are: Sentinel Prevention and Sentinel Banking Intelligence. Sentinel Prevention helps merchants and issuers prevent losses from fraud arising from payment cards. This system claims to prevent fraud from real-time, online and batch approaches (Sentinel product suite for fraud prevention, 2012).

Sentinel Banking Intelligence on the other hand allows its users to obtain fraud related information. Models in this system allow the users to analyze: fraud by country, region, branch and customer category; more frequent channels for carrying out fraud; Fraud time; Fraud concentration by amount; and top business used for fraud. Using the data generated by the Sentinel Banking Intelligence, users of the system can then create rules on the Sentinel Prevention system (Sentinel product suite for fraud prevention, 2012).

Although what has been discussed thus far appears to help diminish fraud, it is not stopping it in its tracks. The techniques currently used by the issuers of payment cards appear to be inefficient. On one hand, fraud needs to occur first. Based on patterns from fraud that has already occurred, rules can then be created to counter fraud containing similar patterns from past fraud. This is a great disadvantage since criminals will always come up with new ways to commit fraud without being detected. Moreover, what about lost or stolen payment cards? It is very easy to charge a legitimate payment card if it was lost or stolen and the cardholder hasn't reported it. Nevertheless, these systems can be used in combination with the systematic queue system from QueuePay which will in turn make QueuePay's customers significantly less prone to fraud.

ENVIRONMENT AND PROCESS FOR PAYMENT CARD TRANSACTIONS

There are two parts to the process for payment card transactions: authorization; and clearing and settlement. This authorization cycle is directly related to the queue system. There are several steps involved in the authorization process. In each of the steps there are players involved. The players in the authorization process are as follows:

- Merchant: Person or entity selling items or services for a profit (wholesale or retail)
- Card Association: Organizations such as Visa, MasterCard, American Express and Discover which validate cardholders' information.
- Issuing Bank: The bank that issues the payment card (with a card logo such as Visa or MasterCard) to the cardholder.
- Acquiring Bank (aka Acquirer): the financial institution that provides a merchant with a merchant account. The acquirer charges a discount rate for processing transactions between the merchant and the issuing bank.
- Front/Back End Processor: Front end processor processes and batches all front end transactions originating from merchants. Back end processor receives batches from front end processors and accepts settlements and, via the Federal Reserve Bank, move funds from the Issuing Bank to the merchant's account.
- Merchant Service Provider: Sets up the merchant with a merchant account and quotes the discount rate. Can be the Acquiring Bank itself. If merchant account was not set up

directly with the Acquiring Bank, the merchant service provider can be a Member Service Provider, Independent Sales Organization or Processor.(Shift4, 1994-2012)

Table 1 provides information about how the payment card authorization process.

Table **1**: Payment Card Authorization Steps (How Merchant Processing Works, 2006-2012)

Step 1	The customer submits his credit card for payment.
Step 2	Merchant receives dollar amount and submits a card transaction to a Payment Gateway (software for e-commerce/online transactions) or Point-of-Sale Terminal (POST, which is a physical terminal/card reader) on behalf of a customer via secure connection.
Step 3	Payment Gateway/POST receives the secure transaction information and passes it via a secure connection to the Merchant Acquirer's Front-End Processor.
Step 4	The Merchant Acquirer's Front-End Processor then sends the authorization request to the card association (Visa or MasterCard).
Step 5	The card association routes the request to the cardholder's issuer.
Step 6	The issuer approves or declines the transaction based on funds availability.
Step 7	The card association forwards the issuer's response to the Merchant Acquirer's Front-End Processor.
Step 8	The Merchant Acquirer's Front-End Processor forwards the response to the Payment Gateway/POST.
Step 9	The Payment Gateway/POST stores the transaction results and sends them to the Merchant.
Step 10	The Merchant receives the authorization response and completes the transaction.

For all these steps to successfully be executed, a technology infrastructure for payment card transactions needs to be in place. This includes networks, databases and middleware. Moreover, all players much comply with the Payment Card Industry Data Security Standards (PCI DSS). By considering the authorization steps for payment card processing, QueuePay will take the role of an issuer. Issuers give the final authorization on availability of funds to card associations to forward authorization confirmation to merchant service providers. QueuePay will be screening authorization requests based on availability of funds in combination of screening queues placed by cardholders. Once the screening for availability of funds and validation of an existing queue, QueuePay will then forward confirmation to the merchant service providers.

THE QUEUEPAY SOLUTION

Despite detection techniques used by merchants, acquirers and issuers to help mitigate the losses, it appears that it is very difficult to prevent fraud solely by using existing techniques. The QueuePay solution prevents fraud before it occurs and before a cardholder's information is compromised. In this system a cardholder's transaction is placed on a queue on QueuePay's servers. The QueuePay data can provide the following information for use internally and by business partners:

- Daily, Weekly, Monthly Total or Average Dollar Value of Transactions.
- Total Number of Transaction in a Given Period.
- Transaction Type Summary.
- Rejected or Unauthorized Charges by Customer Account.
- Rejected or Unauthorized Charges by Merchant.
- Average Queue Quantity by Customer Type per Day, Week and Month.
- Count of Low and High Dollar Value Transactions.

QUEUEPAY IMPLEMENTATION DEMO

Figure 3: QueuePay Transaction Flow

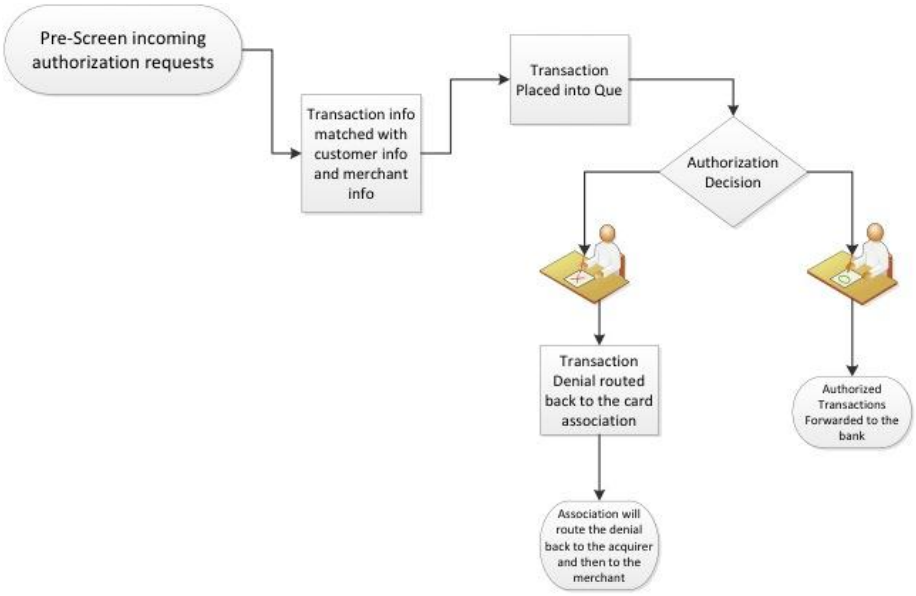


Figure 3 shows the transaction flow of the QueuePay system. First the incoming authorization requests are pre-screened following by matching the cardholder transaction requests with the merchant information. If there approved, the transaction is placed on a queue. Only transactions approved by the cardholder are forwarded to the merchant's bank for further processing.

Figure 4: QueuePay Prototype Relational Model

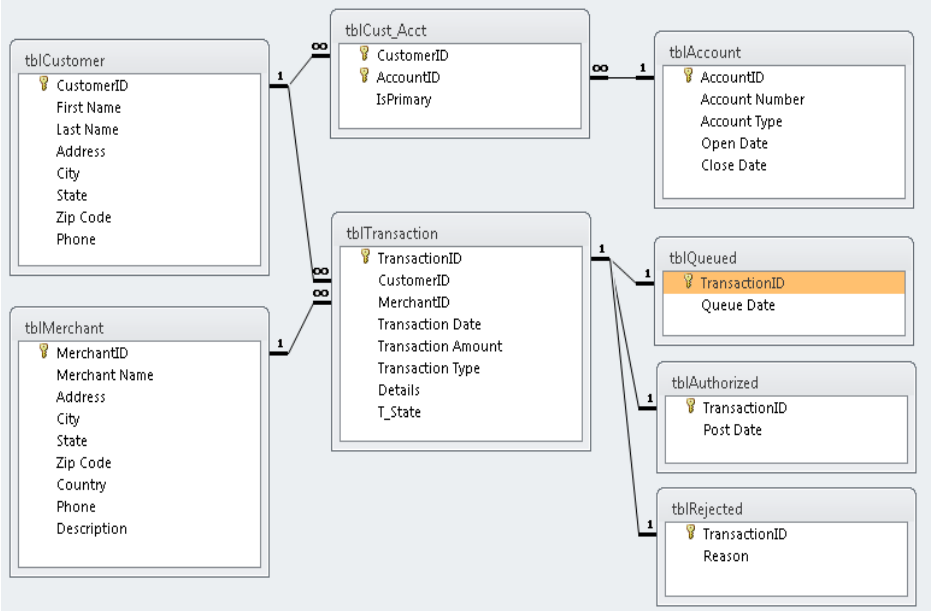
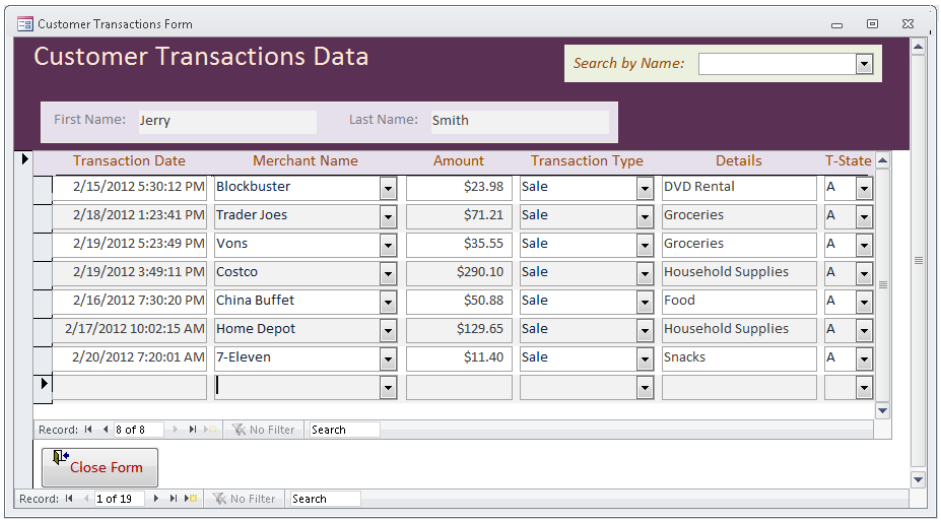


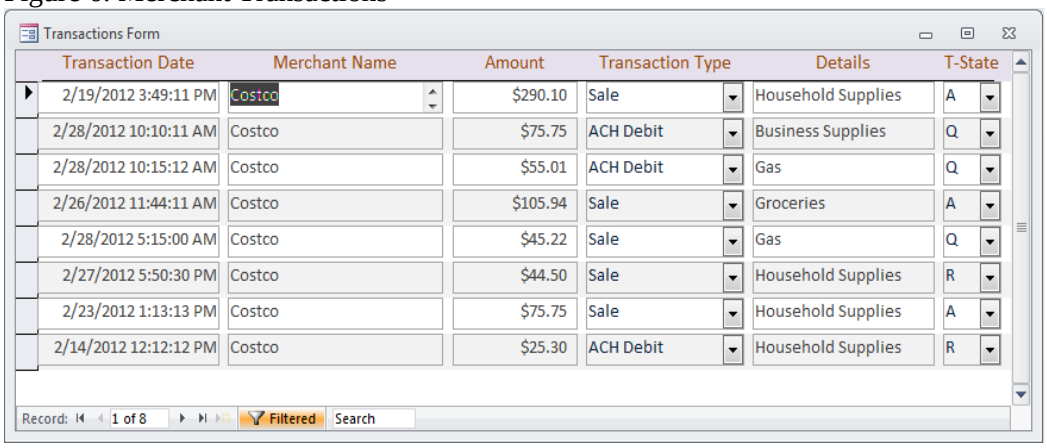
Figure 4 shows a prototype QueuePay relational model with primary keys, fields and relationships. The prototype screen shots were developed using Microsoft Access.

Figure 5: Customer Transactions



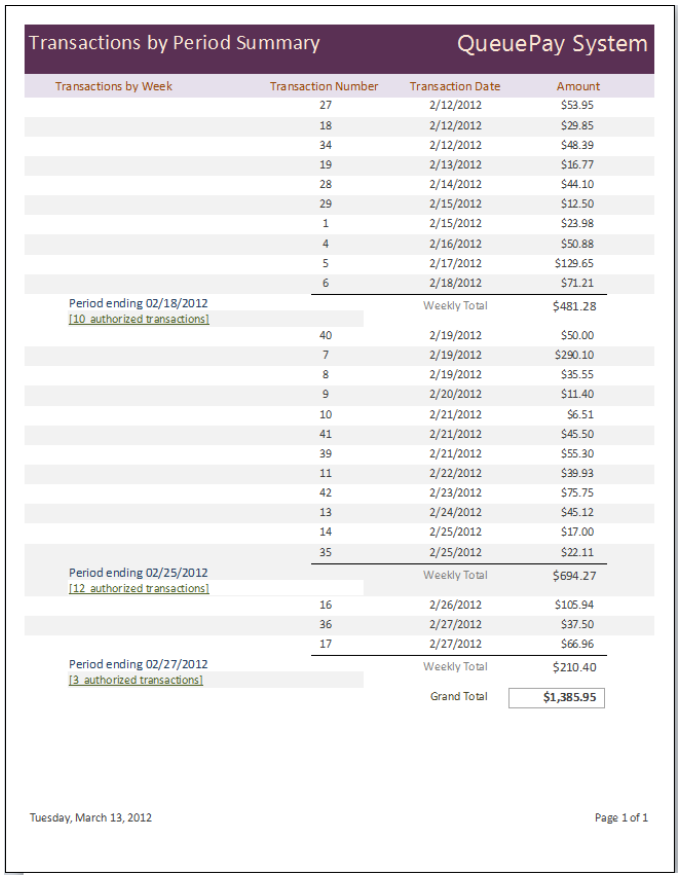
As shown in Figure 5, customer transactions show the Merchant's name, transaction type, details, amount and whether the transaction on QueuePay has been accepted or declined. This allows the QueuePay cardholder to view all of their transactions.

Figure 6: Merchant Transactions



As shown in Figure 6, merchant transactions allow card holders to view a summary of all transactions from each merchant.

Figure **7:** Transactions by Week



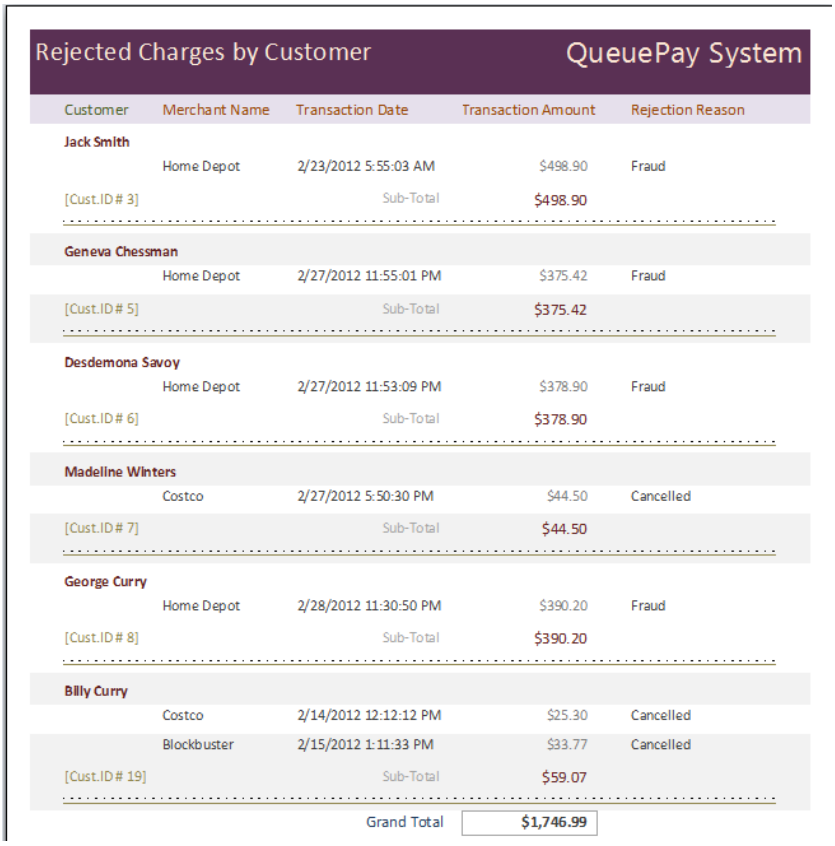
Transactions by Period Summary — QueuePay System

Transactions by Week	Transaction Number	Transaction Date	Amount
	27	2/12/2012	$53.95
	18	2/12/2012	$29.85
	34	2/12/2012	$48.39
	19	2/13/2012	$16.77
	28	2/14/2012	$44.10
	29	2/15/2012	$12.50
	1	2/15/2012	$23.98
	4	2/16/2012	$50.88
	5	2/17/2012	$129.65
	6	2/18/2012	$71.21
Period ending 02/18/2012 [10 authorized transactions]		Weekly Total	$481.28
	40	2/19/2012	$50.00
	7	2/19/2012	$290.10
	8	2/19/2012	$35.55
	9	2/20/2012	$11.40
	10	2/21/2012	$6.51
	41	2/21/2012	$45.50
	39	2/21/2012	$55.30
	11	2/22/2012	$39.93
	42	2/23/2012	$75.75
	13	2/24/2012	$45.12
	14	2/25/2012	$17.00
	35	2/25/2012	$22.11
Period ending 02/25/2012 [12 authorized transactions]		Weekly Total	$694.27
	16	2/26/2012	$105.94
	36	2/27/2012	$37.50
	17	2/27/2012	$66.96
Period ending 02/27/2012 [3 authorized transactions]		Weekly Total	$210.40
		Grand Total	$1,385.95

Tuesday, March 13, 2012 Page 1 of 1

As shown in Figure 7, transactions by week or even monthly are useful for measuring trends and determining periods of high card activity.

Figure 8: Rejected Charges by Customer

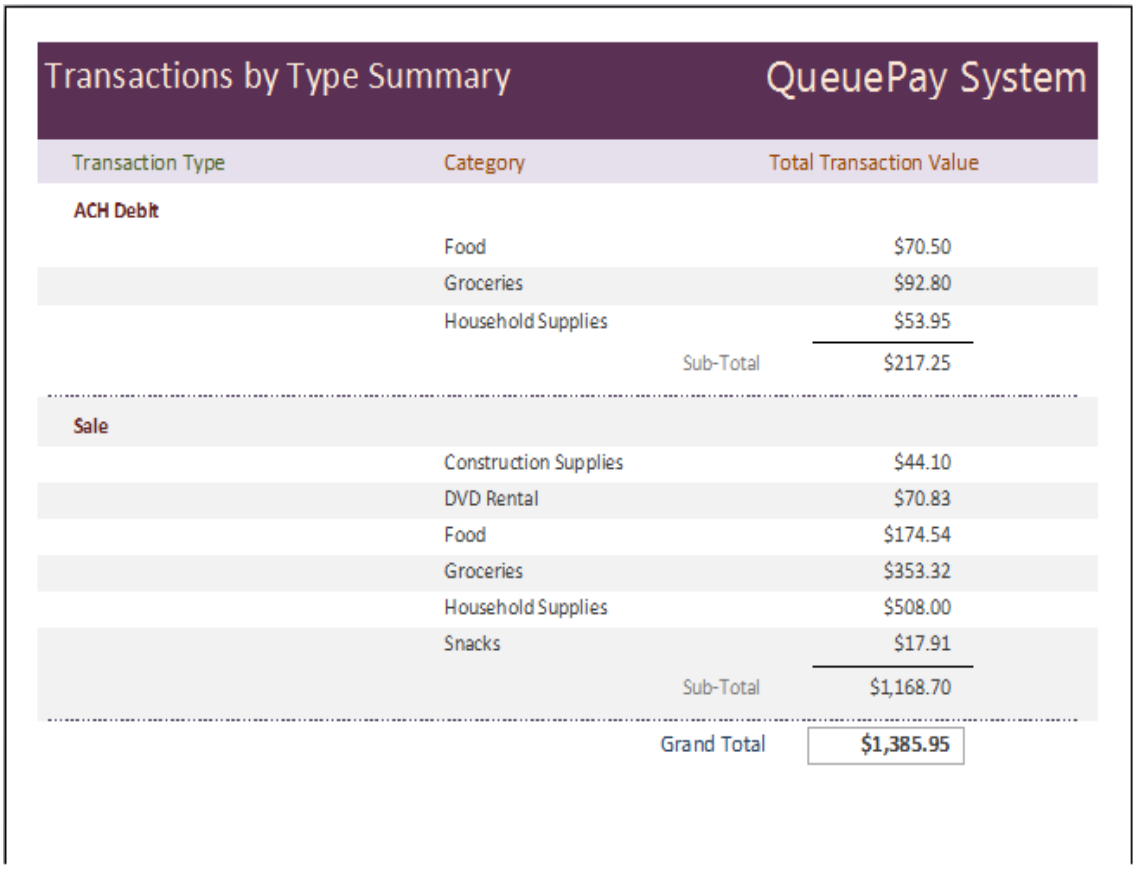


Rejected Charges by Customer — QueuePay System

Customer	Merchant Name	Transaction Date	Transaction Amount	Rejection Reason
Jack Smith				
	Home Depot	2/23/2012 5:55:03 AM	$498.90	Fraud
[Cust.ID # 3]		Sub-Total	$498.90	
Geneva Chessman				
	Home Depot	2/27/2012 11:55:01 PM	$375.42	Fraud
[Cust.ID # 5]		Sub-Total	$375.42	
Desdemona Savoy				
	Home Depot	2/27/2012 11:53:09 PM	$378.90	Fraud
[Cust.ID # 6]		Sub-Total	$378.90	
Madeline Winters				
	Costco	2/27/2012 5:50:30 PM	$44.50	Cancelled
[Cust.ID # 7]		Sub-Total	$44.50	
George Curry				
	Home Depot	2/28/2012 11:30:50 PM	$390.20	Fraud
[Cust.ID # 8]		Sub-Total	$390.20	
Billy Curry				
	Costco	2/14/2012 12:12:12 PM	$25.30	Cancelled
	Blockbuster	2/15/2012 1:11:33 PM	$33.77	Cancelled
[Cust.ID # 19]		Sub-Total	$59.07	
		Grand Total	$1,746.99	

Figure 8 shows transactions that were cancelled because a customer did not place a queue. If the transaction was an error by the customer placing an incorrect queue the rejection reason will show “cancelled”. However, if the customer didn’t place any queue and the customer confirms that the transaction originated by an unknown party, the rejection reason will show “fraud”.

Figure 9: Transaction Type Summary



Transactions by Type Summary — QueuePay System

Transaction Type	Category		Total Transaction Value
ACH Debit			
	Food		$70.50
	Groceries		$92.80
	Household Supplies		$53.95
		Sub-Total	$217.25
Sale			
	Construction Supplies		$44.10
	DVD Rental		$70.83
	Food		$174.54
	Groceries		$353.32
	Household Supplies		$508.00
	Snacks		$17.91
		Sub-Total	$1,168.70
		Grand Total	$1,385.95

Figure 9 shows a summary of transactions based on type. This example shows two transaction types: one originating from a POS or gateway (shown as sale); and the other representing an auto debit (ACH Debit). The report is also programmed to retrieve transaction categories and their respecting totals.

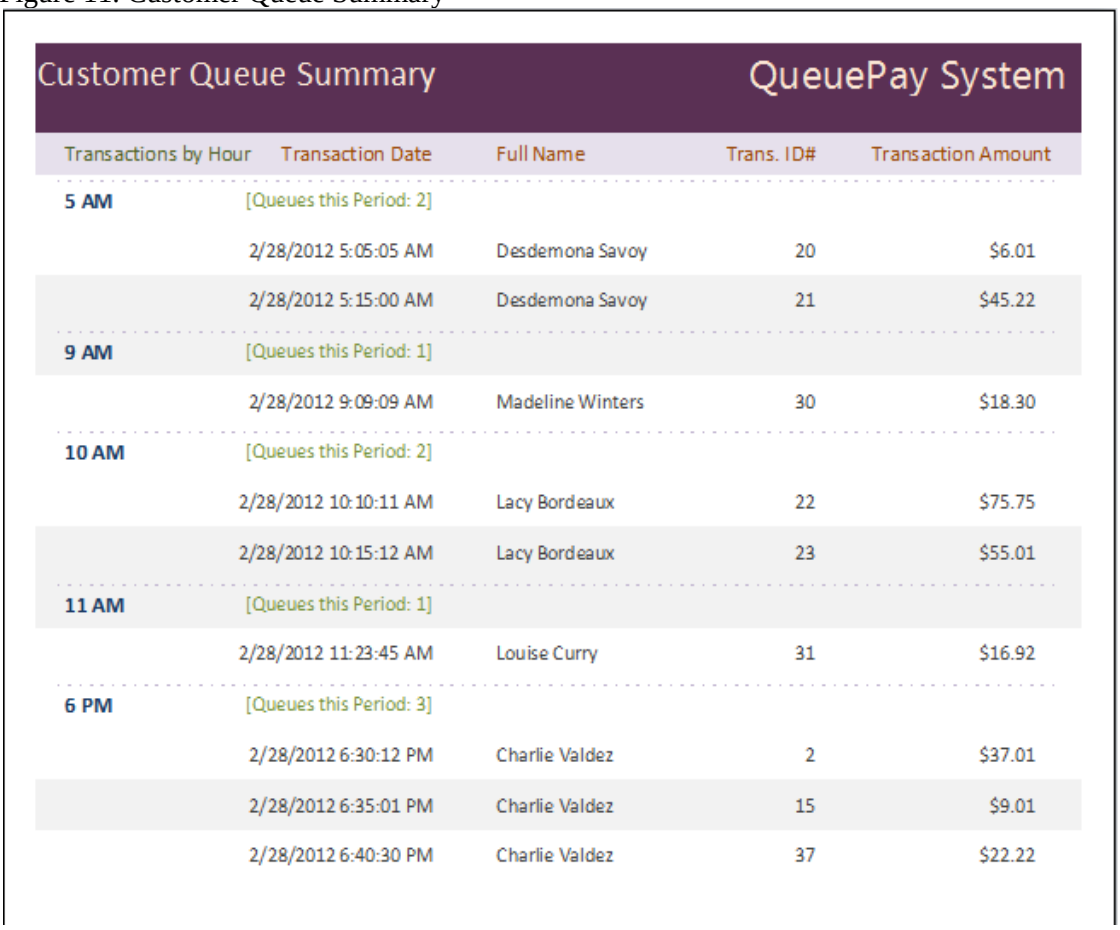
Figure10: Average Low to High Dollar Value Summary

Merchant Transactions Summary — QueuePay System

Merchant Nam	# of Trans.	Total-to-Date	Avg. $ Value	Highest Value	Lowest Value
7-Eleven	2	$17.91	$8.96	$11.40	$6.51
Blockbuster	3	$70.83	$23.61	$29.85	$17.00
China Buffet	3	$116.04	$38.68	$50.88	$16.77
Costco	3	$471.79	$157.26	$290.10	$75.75
Home Depot	4	$240.20	$60.05	$129.65	$12.50
Rock N Roll Sushi	3	$129.00	$43.00	$66.96	$22.11
Trader Joes	4	$217.13	$54.28	$71.21	$45.12
Vons	3	$123.05	$41.02	$50.00	$35.55

Figure 10 allows users to retrieve information on merchant transaction high and low values, their average, and year to date amounts. The report also provides the user with a count of transactions per merchant.

Figure 11. Customer Queue Summary



Customer Queue Summary — QueuePay System

Transactions by Hour	Transaction Date	Full Name	Trans. ID#	Transaction Amount
5 AM	[Queues this Period: 2]			
	2/28/2012 5:05:05 AM	Desdemona Savoy	20	$6.01
	2/28/2012 5:15:00 AM	Desdemona Savoy	21	$45.22
9 AM	[Queues this Period: 1]			
	2/28/2012 9:09:09 AM	Madeline Winters	30	$18.30
10 AM	[Queues this Period: 2]			
	2/28/2012 10:10:11 AM	Lacy Bordeaux	22	$75.75
	2/28/2012 10:15:12 AM	Lacy Bordeaux	23	$55.01
11 AM	[Queues this Period: 1]			
	2/28/2012 11:23:45 AM	Louise Curry	31	$16.92
6 PM	[Queues this Period: 3]			
	2/28/2012 6:30:12 PM	Charlie Valdez	2	$37.01
	2/28/2012 6:35:01 PM	Charlie Valdez	15	$9.01
	2/28/2012 6:40:30 PM	Charlie Valdez	37	$22.22

Figure 11 shows the transactions by the hour. This also helps measure peak use time by customer.

Figure 12: Consolidated Queries

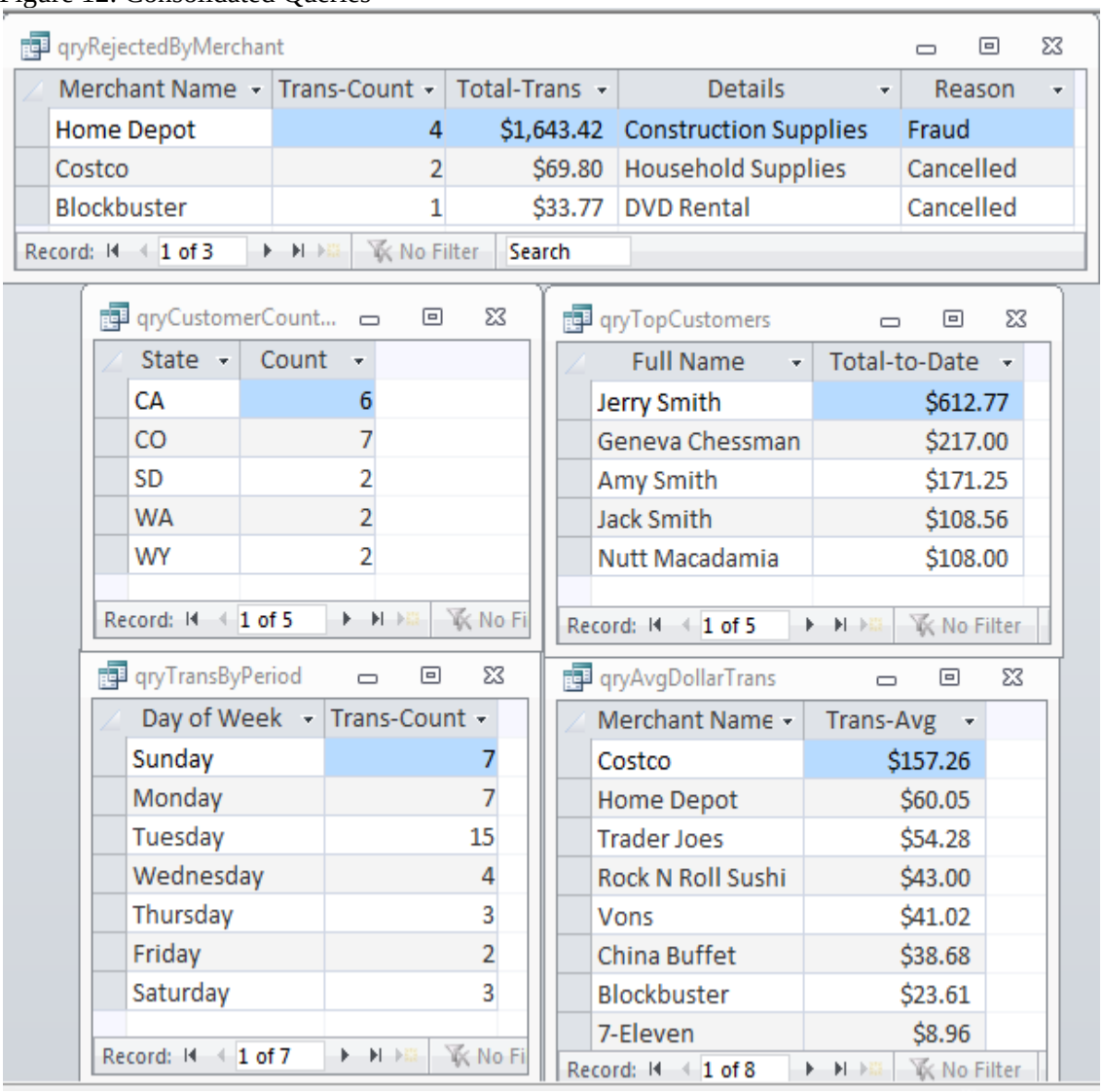


Figure 12 shows the ability of the QueuePay system to provide consolidated information for use internally and by business partners.

SUMMARY

This paper analyzed the industry of payment cards, the emergence of the problem, and demonstrates that the solution to the problem doesn't require information technology capabilities beyond what's available today. It is acknowledged that: payment card fraud is a growing problem and the proposed solution is not only effective but also highly lucrative. QueuePay's system will provide value to the industry by: significantly reducing losses related to fraud; increasing cardholders' trust and therefore encourage more payment card usage; reducing the discount rate for merchants who partner with QueuePay; giving cardholders the means to have total control of their account balances; creating new marketing affiliations with QueuePay's advertising capabilities.

REFERENCES

(2008, March). *The Nielson Report* (889).

Alidina, S., Austin, G., & Barber, J. a. (2009-2012). *World Payments Report.* Capgemini, RBS and EFMA.

Arora, N., Dreze, X., Ghose, A., & Hess, J. (2008). "Putting One-to-One Marketing to Work: Personalization, Customization, and Choice." *Marketing Letters* , 305-321.

Bhatla, P., Prabhu, V., & Dua, A. (2003, Jun). "Understanding Credit Card Frauds." *Cards Business Review* .

Breuer, R., & Brettel, M. (2012). "Short- and Long-term Effects of Online Advertising: Differences between New and Existing Customers." *Journal of Interactive Marketing* (26), 155-166.

Carbone, J. A. (2008). *IT Architecture Toolkit.* Upper Saddle River, NJ: Prentice Hall.

Council, P. S. (Ed.). (2011, May). "PCI DSS Prioritized Approach for PCI DSS 2.0."

Credit Card Processing Fees & Rates. (2011). Retrieved May 5, 2012, from www.cardfellow.com: http://www.cardfellow.com/blog/credit-card-processing-fees/

Ekrem, D., & Ozcelik, H. (2011). "Detecting credit card fraud by genetic algorithm and scatter search." *Expert Systems with Applications* , 13057-13063.

Guide for Groups Interested in Chartering a State Bank in California. (n.d.). Retrieved October 2012, from State of California Department of Financial Institutions: www.dfi.ca.gov/cacharter/guide.asp

Hardekopf, B. (2010, May). "The History of Credit Cards." *Business Credit* , pp. 50-51.

How Merchant Processing Works. (2006-2012). Retrieved Apr 25, 2012, from www.ippay.com: http://www.ippay.com/index.php?q=merchant_processing_overview

Iyer, G., Soberman, D., & Miguel, J. (2005). "The Targeting of Advertising." *Marketing Science* , 461-476.

PCI Quick Reference Guide. (2008). PCI Security Standards Council.

Privacy Commissioner. (2007). *Report of an Investigation into the Security, Collection and Retenition of Personal Information: TJX Companies Inc./Winners Merchant international L.P.* Alberta, Canada: Office of the Privacy Commissioner of Canada.

Robertson, D. (2011, Nov 21). "U.S Leads the World in Credit Card Fraud, states The Nilson Report." *Business Wire* .

Sachdeva, P. a. (2011, Mar 10). "Data Mining using Learning Techniques for Fraud Detection." *Bharati Vidyapeeth's Institute of Computer Applications and Management* .

Sentinel product suite for fraud prevention. (2012). Retrieved Apr 25, 2012, from http://www.smartsoftint.com/eng/products.html

Shift4. (1994-2012). *Players*. Retrieved 2012, from Shift4: www.shift4.com

Sylvester, O. (2012). Transnational Credit Card Fraud. Retrieved Apr 15, 2012, from http://people.exeter.ac.uk/watupman/undergrad/owsylves/index.html