



**Snohomish County  
Office of the County Performance Auditor**

**AUDIT OF SNOHOMISH COUNTY'S  
RECEIPT OF PAYMENT CARDS AND E-PAYMENTS**

**May 28, 2008**

**Performance Auditor:**

Kymber Waltmunson

**Project Team:**

Connie Barndt

Lea Fortmann

Kymber Waltmunson

(425) 388-3006  
FAX (425) 258-9439  
M/S #302  
3000 Rockefeller Avenue  
Everett, Washington 98201-4046



## TABLE OF CONTENTS

<b>1 INTRODUCTION</b>	<b>- 3 -</b>
A. SUMMARY OF RESULTS	- 3 -
B. NOTES	- 3 -
C. STRENGTHS AND CHALLENGES	- 2 -
D. COSTS AND BENEFITS OF PAYMENT CARDS	- 2 -
E. COUNTY USE OF E-PAYMENT AND PAYMENT CARDS	- 3 -
<b>2 MANAGEMENT</b>	<b>- 6 -</b>
<b>The County has taken action to improve management of electronic and payment card processes.</b>	<b>- 6 -</b>
A. SET DIRECTION AND PROVIDE EXPERTISE	- 6 -
B. EFFECTIVELY TRAIN STAFF	- 6 -
C. PERFORM LEGAL DUE DILIGENCE	- 7 -
<b>3 SECURITY</b>	<b>- 8 -</b>
<b>The County has enhanced security practices and there are further opportunities for action.</b>	<b>- 8 -</b>
A. ESTABLISH, COMMUNICATE, AND MEET EXPECTATIONS	- 8 -
B. SECURE SENSITIVE DATA	- 8 -
<b>4 AUDIT RESPONSE</b>	<b>- 10 -</b>
<b>5 APPENDICES</b>	<b>- 12 -</b>
Appendix A: Objectives, Scope and Methodology	- 12 -
Appendix B: Officials Interviewed and Consulted	- 13 -
Appendix C: Payment Card Industry Data Security Standards (PCI-DSS)	- 15 -
Appendix D: National Electronic Commerce Coordinating Council (EC <sup>3</sup> )	- 16 -
Appendix E: Interchange	- 17 -
Appendix F: Per-Transaction Fees	- 18 -



## 1 INTRODUCTION

### A. SUMMARY OF RESULTS

Snohomish County departments and offices first started accepting payment cards for county fees and services in 1998 and internet payment tools to accept payments online in 2003. In 2007 the county accepted nearly \$15 million in revenues via payment cards. New challenges and responsibilities come with the acceptance of payment cards.

The county utilized this audit as an opportunity to ensure that their payment card and e-payment practices are effective. Significant progress was made over the course of the audit improving policy guidance, becoming familiar with the costs of accepting payment cards, understanding and implementing Payment Card Industry Data Security Standards (PCI-DSS), and assessing and advancing information security.

Snohomish County is continuing its work on effective execution of policies across the county, developing and implementing information security awareness and other ongoing training, and validating PCI-DSS compliance.

### B. NOTES

#### ***Government Auditing Standards Compliance Statement***

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.<sup>1</sup>

Government auditing standards require that any impairments or appearance of an impairment to independence be disclosed. In 2007, the Office of the County Performance Auditor transitioned from organizational placement in the Auditor's Office to the County Council. In addition, during the course of this audit a staff member of the Office of the County Performance Auditor was hired into a management role in the Auditor's Office. Results of e-commerce and point of sale acceptance of payment cards from the Auditor's Office were included in this audit but were not the sole source of evaluation.

---

<sup>1</sup> See Appendix A for audit objectives, scope, and methodology.



### ***Auditee Communications***

Interim reports and other early communications regarding audit findings were forwarded to departments to allow the department to begin to resolve issues in a timely manner. Management letters were provided as a supplement to this report.

## **C. STRENGTHS AND CHALLENGES**

During evaluation of receipt of payment cards and e-payments noteworthy strengths and the challenges facing the county were identified.

### ***Strengths:***

- During the course of the audit efforts were made across the county to meet payment card best practices. In most cases, information security issues were resolved within days of management and staff becoming aware of identified issues.
- Senior management has played a role in e-payment and payment card planning as part of their department and office strategic business goals.
- Federal, State, and local laws have been considered in implementation of electronic and payment card processes.
- Departments and offices report that they are satisfied with their e-payment websites and that use of their online payment programs has exceeded their expectations.

### ***Challenges:***

- Compliance requirements from the credit card industry are complex and can be interpreted differently depending on the source of information.
- The dispersed nature of payment card processing makes ensuring consistent practice across the county difficult.

This audit utilized a combination of criteria from Payment Card Industry Data Security Standards (PCI-DSS) and the Electronic Commerce Coordinating Council (EC<sup>3</sup>).<sup>2</sup> PCI-DSS is required for Snohomish County and EC<sup>3</sup> promulgates best practices.

## **D. COSTS AND BENEFITS OF PAYMENT CARDS**

Snohomish County and other governments are making efforts to streamline services and are responding to customer demand for ways to conduct business with payment cards. There are costs and benefits to be evaluated when implementing new payment acceptance channels.

---

<sup>2</sup> More information regarding the audit's objectives, scope, and methodology can be seen in Appendix A and details about PCI-DSS and EC<sup>3</sup> in Appendices C and D.



### ***Over-the-Counter Payment Card Benefits***

Over time, the benefits of accepting payment cards may include:

- reduced risk and costs associated with processing cash and checks;
- reduced risk and costs associated with processing NSF<sup>3</sup> checks;
- fewer errors and lost transactions;
- faster fund deposit and availability at the bank; and
- increased opportunity for process automation.

### ***E-Payment Benefits***

As e-payment processes are put into place and utilized by customers benefits may include:

- decreased phone and over-the-counter traffic;
- decreased mail processing costs;
- increased customer access to services; and
- improved turnaround time for customers.

### ***Costs***

The costs of accepting payment cards both over the internet and over-the-counter may include:

- new/increased transaction charges and merchant fees;
- increased costs due to multiple departments processing cards;
- ensuring that staff maintain new skill sets, business processes, and controls to mitigate risks; and
- establishing and maintaining security standards.

## **E. COUNTY USE OF E-PAYMENT AND PAYMENT CARDS**

Snohomish County is beginning to invest in internet and payment card payment systems. There are currently five departments and offices that accept internet payments and seven that accept payment cards over the counter. Many departments and offices accept cash and checks only.

---

<sup>3</sup> Non-Sufficient Funds



Figure 1

Accept Payment Over the Internet	Accept Credit/Debit Card Payment Over the Counter	Accept Only Cash or Checks*
Auditor	Airport	Assessor
District Court	Auditor	BRB, BOE
Finance	**Clerk	Corrections
Parks	District Court	County Council
Planning and Development	Facilities	Human Services
	Parks	Information Services
	Planning and Development	Medical Examiner
		Office of Public Defense
		Performance Auditor
		Prosecuting attorney
		Public Works
		Sheriff
		***Treasurer

Source: Snohomish County Office of the County Performance Auditor

\*Some departments and offices are not included above because they do not accept payments

\*\* The Clerk's Office is currently developing a process to accept payments over the internet for legal financial obligations and other Clerk services.

\*\*\*The Treasurer is currently developing a process to accept e-payments and payment cards for property taxes

Figure 2

Department or Office	Payment Cards Accepted		Services with Payment Card Option
	Internet	Over the Counter	
Airport		X	Hangar rent, other fees
Auditor	X	X	Many licensing, recording, and elections services
Clerk		X	All clerk services
District Court	X	X	Fines and fees
Facilities		X	Parking
Finance	X		Arts donations, Focus on Farming Conference
Parks	X	X	Day parking, pool entry, rentals, class registrations
PDS	X	X	Some Permits, Developer's Breakfast

Source: Snohomish County Office of the County Performance Auditor



**Internet Payment Card Use**

The county's three e-payment processors (vendors who directly accept payment card information online, route it through the bank, then pay the county) handled 22,694 customer transactions for the county in 2007, up 219% from 7,113 transactions in 2006.

Figure 3

**Over the Counter Payment Card Use**  
Seven departments and offices

Internet Payment Card Processor	Department/Office	2006 Revenue	2007 Revenue
Cybersource	Auditor, District Ct, Finance, PDS	\$348,000	\$2,560,000
Active	Parks	\$335,000	\$350,000
MyBuildingPermit	PDS	\$96,000	\$69,000
<b>TOTAL</b>		<b>\$779,000</b>	<b>\$2,979,000</b>

accept payment cards over the counter or over the telephone. Data comparing 2006 to 2007 payment card revenues over the counter was not available.

Figure 4

Department/Office	2007 Over-the-Counter Payment Card Revenue
Airport	\$387,000
Auditor	\$293,000
Clerk	\$489,000
District Court	\$417,000
Facilities	\$88,000
Parks	\$438,000
Planning	\$9,810,000
<b>TOTAL</b>	<b>\$11,922,000</b>

Source: Snohomish County Office of the County Performance Auditor

**Cash or Check Only**

Opportunities to utilize internet and/or over-the-counter payment cards were identified in each department and office that accepts customer payments. Departments and offices that have implemented payment card options report that customers have responded positively. Some believe that expanded payment options have contributed to increases in revenues<sup>4</sup>.

<sup>4</sup> The auditors could not verify a causal relationship between expanded payment options and increases in revenues due to multiple variables occurring simultaneously.



## 2 MANAGEMENT

Strong management of electronic and payment card processes will ensure that they are effective, efficient, meet laws and regulations, and will have long-term viability.

### ***Issue 1: The County has taken action to improve management of electronic and payment card processes.***

#### A. SET DIRECTION AND PROVIDE EXPERTISE

##### ***Set Direction for Department/Office-level Programs***

###### Process Management

Basic coordination between Finance, the Treasurer's Office, and Department of Information Services regarding implementation of new departmental payment processes was evident in initial audit evaluation. Finance has taken the lead on e-payment and payment card process design and performance. This leadership will help ensure that current processes are sustained and that future opportunities for improvement are identified.

###### Policy

Finance Policy 1140 "Receipt of Electronic & Credit/Debit Card Payments" has been developed. These policies have led to improved electronic and payment card processes. As departments and offices develop new channels for customer payment they will have guidance for effective and secure processes.

###### Policy Implementation

Special effort was made by Finance to effectively communicate Finance Policy 1140 to departments and offices, and although departments report that they understand policy requirements, some gaps in implementation were observed. Most policy components have been successfully put into operation in the majority of departments and offices. Effective payment card practices are discussed further in chapter 3, section B.

#### B. EFFECTIVELY TRAIN STAFF

##### ***Communication of Processes, Regulations, and Technologies***

New processes have been developed to promote adequate competencies across departments and offices and to provide evidence of training. It will be important to ensure that process updates and other information is effectively communicated both to department and office management and to line-level staff who process and document payment card transactions. Staff in Finance, the Treasurer's Office, and Department of Information Services should stay abreast of emerging regulations and technologies and should provide periodic updates to staff in departments and offices.





### ***Understand and Fund Costs***

Departments and offices accepting payment cards are now aware of the costs associated with accepting payment cards; however, initial interviews showed that these costs were not fully understood by some staff in some departments. In order to make informed and effective policy choices, department- and office-level decision-makers must be aware of the detailed and complex information regarding interchange rates, transaction fees, convenience fees, and costs/benefits of different card types. The Treasurer has identified cost information to provide to departments or offices considering accepting payment cards or internet payment options.

Costs to accept payment cards may include:

- Interchange<sup>5</sup> rates
- Per-transaction fees<sup>6</sup>
- Magnetic stripe reading equipment rental or purchase costs
- PIN pad rental or purchase costs
- Merchant account setup and maintenance fees
- Marketing costs

### **C. PERFORM LEGAL DUE DILIGENCE**

Finance, the Treasurer, and the Department of Information Services have begun broader consultation with the Prosecuting Attorney's Office<sup>7</sup>. The National Electronic Commerce Coordinating Council (EC<sup>3</sup>) maintains that involving legal counsel may help prevent problems and increase the likelihood of a successful e-commerce system. Legal input into planning helps ensure that departments and offices have sufficient legal advice on issues such as legal impediments to the county's processes, understanding of current and emerging laws, and defensibility of payment disputes.

Websites should contain statements reviewed by the Prosecuting Attorney's Office establishing the intended purpose and legal use of the site; describing all parties' rights and responsibilities; and privacy practices of the county. The county has privacy statements displayed on payment websites and is developing additional information to post.

#### **Recommendation 1:**

Snohomish County Finance/Treasurer/DIS should continue to implement new management processes related to e-payment and payment cards including:

- setting direction and providing expertise;
- effectively training staff; and
- performing legal due diligence.

<sup>5</sup> See Appendix E for more information on interchange.

<sup>6</sup> See Appendix F for more information on per-transaction fees.

<sup>7</sup> Previous consultation included a 2004 version of the privacy statement and approval of contracts as to form.



### 3 SECURITY

Employing adequate safeguards ensures that cardholder information is protected against unauthorized use, disclosure, modification, damage or loss.

#### ***Issue 2: The County has enhanced security practices and there are further opportunities for action.***

##### A. ESTABLISH, COMMUNICATE, AND MEET EXPECTATIONS

###### ***Payment Card Industry Data Security Standard (PCI-DSS) Compliance***

Compliance with PCI-DSS<sup>8</sup> is required of Snohomish County and any other merchant who accepts payment cards. To put this requirement in context, many merchants and jurisdictions are currently focusing on complying with PCI requirements but relatively few have met the standards to date. During the course of the audit, the county took full responsibility for compliance with PCI-DSS and plans to submit the PCI self-assessment questionnaire validating compliance by September 2008.

###### ***Information Security Awareness Program***

Snohomish County has some information security awareness tools in place and the security awareness program required by PCI-DSS is in the planning stages. A formal security awareness program will educate all employees about the importance of cardholder data security. Finance Policy 1140 has been communicated to department and office management who have, in turn, communicated the policy to line staff. Department of Information Services has developed an information security handbook and training, but it does not include information regarding cardholder data and over the counter security practices.

##### B. SECURE SENSITIVE DATA

###### ***Over the Counter Transactions***

Procedures have been put in place to ensure that cardholder data collected prior to implementation of Finance Policy 1140 is adequately protected. In many cases cardholder information has been redacted or destroyed. In early audit evaluation some departments and offices did not meet all PCI-DSS standards. Finance Policy 1140 now requires adequate security in conformance with PCI-DSS standards. Compliance with the policy has resulted in protection of cardholder data. Departments and offices no longer retain any cardholder information beyond the time it takes to complete a transaction.

Auditors made three visits to departments and offices accepting payment cards, the first occurred in December 2007 and the second and third occurred in May

<sup>8</sup> See Appendix C for more information about PCI-DSS.



2008. Results of each observation were communicated to departments/offices.

Primary areas of evaluation based on PCI-DSS requirements included:

- Are there effective security policies and security training?
- Is sensitive cardholder data securely documented, stored, and transmitted?
- Are card validation codes stored?
- Is access to sensitive data limited?
- Is sensitive information stored electronically?

#### Enhancements

A review of payment card practices at the second and third observation dates showed advances in security of cardholder data:

- Finance Policy 1140 has been communicated and is available to staff.
- All county payment card equipment has been evaluated to ensure secure transmission to financial institutions.
- Equipment is upgraded and has been replaced to ensure that both merchant and customer receipts do not include full credit card numbers.
- No card validation codes are stored.
- Access to sensitive data has been limited to a small number of staff.
- Departments and offices redacted, eliminated, and secured sensitive data.
- A DIS evaluation gives reasonable assurance that there is no electronic storage of information on the county's system.

#### ***E-Commerce Transactions***

By using third party credit card processing contractors for online transactions and monitoring the equipment used to send payment card data to the processors, the county avoids processing and storing sensitive information electronically and being responsible for its security.

#### Recommendation 2:

Snohomish County Finance/Treasurer/DIS should submit the PCI-DSS Self-Assessment Questionnaire validating compliance with the standard by September as planned.

#### Recommendation 3:

Snohomish County Finance/Treasurer/DIS should continue development and implementation of a countywide information security awareness program that includes payment card security information.



## 4 AUDIT RESPONSE

No.	Recommendation	Management Response			Implementation Status	
		Concur	Partially Concur	Do Not Concur	Underway	Planned
1	Snohomish County Finance/Treasurer/DIS should continue to implement new management processes related to e-payment and payment cards including: <ul style="list-style-type: none"> <li>• setting direction and providing expertise;</li> <li>• effectively training staff; and</li> <li>• performing legal due diligence.</li> </ul>	✓			✓	
2	Snohomish County Finance/Treasurer/DIS should submit the PCI-DSS Self-Assessment Questionnaire validating compliance with the standard by September as planned.	✓			✓	
3	Snohomish County Finance/Treasurer/DIS should continue development and implementation of a countywide information security awareness program that includes payment card security information.	✓			✓	

May 23, 2008

Ms. Kymber Waltmunson  
Snohomish County Performance Auditor  
3000 Rockefeller Avenue  
Everett, WA 98201

### Re: Performance Audit of Receipt of Payment Cards and E-Payments

Dear Ms. Waltmunson:

Thank you for the opportunity to review and respond to the May 14, 2008 draft performance audit report of Snohomish County's receipt of payment cards and e-payments. We appreciate that your audit team invested significant time to gain an understanding of PCI compliance requirements and the County's related receipting processes and controls. It is the goal of the Finance Department, the Department of Information Services (DIS) and the Office of the County Treasurer to provide the payment options desired by our customers while ensuring those processes are cost effective, efficient and secure.

We provide this letter of response pursuant to SCC 2.700.060.




Recommendation 1 encourages Snohomish County Finance, Treasurer's Office and DIS to continue implementing new management processes related to e-payment and payment cards including setting direction and providing expertise, effectively training staff and performing legal due diligence. Snohomish County Finance, Treasurer and DIS staff are continuing to work cooperatively with each other through timely sharing of information related to continually changing e-payment technology and PCI requirements. This cooperation will continue. Policies and processes are being, and will be, modified accordingly and departmental staff apprised and trained as appropriate. We will continue to perform legal due diligence as has consistently been done in the past.

Recommendation 2 encourages Snohomish County Finance/Treasurer/DIS to submit the PCI-DSS Self-Assessment Questionnaire validating compliance with the standard by September. Snohomish County Finance, Treasurer and DIS staff have assessed compliance and fully intend to file a completed report by September 2008.

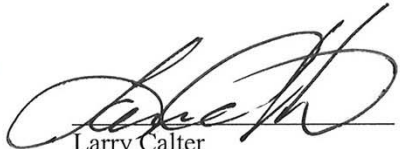
Recommendation 3 encourages Snohomish County Finance, Treasurer's Office and DIS to continue development and implementation of a countywide information security awareness program that includes payment card security information. Snohomish County Finance policy currently requires all staff engaged in e-payment and payment card receipting processes to be properly trained. The policy emphasizes security of customer data as being of paramount importance. In addition, DIS currently provides security training at new employee orientation. Management staff from these departments will explore the possibilities of providing additional training to those directly involved in the receipting processes.

In closing, we thank you and your team for the efforts made to provide information to aide the County in improving processes. As encouraged by you, staff from Snohomish County Finance, the Snohomish County Treasurer's Office and the Department of Information Systems will continue to work closely together to ensure the public is provided the payment options they desire in a cost effective manner and highly secure environment.

Sincerely,

  
Roger Neumaier  
Director of Finance

  
Kirke Sievers  
County Treasurer

  
Larry Calter  
Director of Information Services



## 5 APPENDICES

### 5.1 *Appendix A: Objectives, Scope and Methodology*

This audit focused on the receipt of payment by county departments or vendors for which the county manages receipts and evaluated credit and debit card payments received via internet, phone, fax, and point-of-sale. Status was evaluated during the period from November 2007 to May 2008 with analysis of past data for reference. Objectives and the section of the report where they are described are shown in Figure 5.

Figure 5

OBJECTIVES	Sub-Category	REPORT SECTION
Background		1
Determine if Snohomish County has adequate development, implementation, and management processes in place to ensure effective receipt of e-payments and payment card payments.	Management	2
	Privacy and Security	3

The methods used to gather information included:

1. Review of Snohomish County documents
2. Electronic data analysis (if any)
3. Information system process analysis
4. Review of Laws, Regulations, Guidelines etc.
5. Interviews<sup>9</sup> with:
  - a. Snohomish County officials
  - b. Snohomish County department management
  - c. Snohomish County department and office staff
  - d. Other jurisdictions
  - e. Vendors
6. Literature<sup>10</sup> review (internet, studies, publications)
7. Observation of Snohomish County processes

<sup>9</sup> See Appendix B for detail.

<sup>10</sup> See Appendix C for detail.



## 5.2 *Appendix B: Officials Interviewed and Consulted*

### County Staff

#### *Finance*

1. Roger Neumaier, Finance Director
2. Sharyl Raines, Controller

#### *Executive's Office*

3. Mark Soine, Deputy Executive

#### *Information Services*

4. Larry Calter, Director
5. Ron Knight, Applications Manager
6. Dave Hopkins, Systems Supervisor
7. Tom Hartley, Information Security Engineer
8. John Hartwig, Deputy Director
9. Lisa Hall, Records Management Supervisor

#### *Treasurer's Office*

10. Kirke Sievers, Treasurer
11. Jerry Lindsey, Accounting Manager
12. Debi Putnam, Chief Deputy Treasurer

#### *Auditor's Office*

13. Carolyn Diepenbrock, Auditor
14. Carolyn Ableman, Chief Deputy Auditor
15. Connie Barndt, Chief Deputy Auditor
16. Vicki Lubrin, Licensing Manager
17. Ute Padilla, Licensing Supervisor
18. Diane Mickunas-Ries, Recording Manager
19. Shelley LaCasse, Recording Supervisor

#### *Prosecuting Attorney*

20. Jason Cummings, Chief Civil Deputy Prosecuting Attorney
21. Jim Rucci, Budget and Fiscal Administrator

#### *Planning Development Services*

22. Carol Taber, Accounting and Financial Services Manager
23. Mick Watson, Fiscal Resources Analyst
24. Barb Mock, Administrative Manager, Business Processes and Technology
25. Holly Faller, Supervisor, Customer Support Center
26. Chris Fenner, Accounting Technician

#### *District Court*

27. Linda Diemert, Everett Division Supervisor
28. Paulette Revoir-Beegle, Assistant Director
29. Pam Haley, Legal Process Assistant
30. Steve Brown, Director, District Court Administration

#### *Clerk's Office*

31. Kathleen Gunn, Chief Deputy Clerk
32. Anne Trice, Manager, Customer Service and Judicial Finance





*Airport*

27. Susan Kern, Business Manager

*Parks*

- 33. Bridgid Smith, Administrative Services Manager
- 34. Carla Kneeland, Accountant
- 35. Kay Akerlund, Capital Funds Specialist
- 36. Jessica Warner, Office Assistant
- 37. Christy Hill, Administrative Specialist, Evergreen Fair

*Facilities Management*

- 38. Karla Beers, Administrative Specialist
- 39. Al Garcia, Administrative Operations Manager

*Human Services*

40. Mike Fulcher, Division Manager

*Sheriff's Office*

41. Joanie Fadden, Fiscal Resources Analyst

*BRB/BOE*

42. Marsha Carlsen, Clerk

*Corrections*

43. Deborah Payne, Administrative Operations Coordinator

*Assessor's Office*

44. Linda Hjelle, Chief Deputy Assessor

*Public Works*

- 45. Allen Mitchell, ER&R Fleet Equipment Manager, Fleet Management
- 46. Steve Torrence, Fiscal Resource Analyst
- 47. Deanna Clark Willingham, Real Property Supervisor
- 48. Sue Ruth, Accounting Technician, Solid Waste

*Medical Examiner*

49. Carolyn Sanden, Deputy Director

*Office of Public Defense*

50. Kristin Crane, Interviewer Supervisor

Other

- 51. Lisa Rhodes, Vice President, Senior Account Manager, Bank of America
- 52. Bom Lee, Sales Director, First Data Commercial Services (associated with Frontier Bank)
- 53. Gary Clawson, Information Services, Bellevue, WA
- 54. John Backman, Executive Director, eCityGov Alliance
- 55. Mike Hamilton, Chief Information Security Officer, City of Seattle, Washington
- 56. Bob Dantini, former Snohomish County Treasurer
- 57. Tyson/Tyler, Technical Support, Security Metrics





### 5.3 *Appendix C: Payment Card Industry Data Security Standards (PCI-DSS)*

Payment Card Industry Data Security Standards, called PCI-DSS or most often simply PCI, are promulgated by the PCI Security Standards Council- a group founded by credit card companies. Their website states, “The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.” Credit card companies require compliance with PCI but pass on the responsibility for ensuring compliance to banks, often called “acquirers”, who in turn often pass on responsibility to third party “qualified security assessors” (QSAs).

Merchants fall into one of four levels of PCI compliance that depend on the number of credit card transactions processed through e-commerce and/or over the counter. Depending on merchant level, compliance includes completion of a self-assessment questionnaire, quarterly network scans by an “approved scanning vendor” (ASV), and/or a self-assessment questionnaire validated by a QSA. Compliance with PCI and acceptance of the self-assessment questionnaire is ultimately determined by the acquiring bank.

Failing to comply with PCI standards could result in costly fines and legal liability, restrictions on acceptance of payment cards, withdrawal of authority to accept payment cards, and loss of public trust.

PCI compliance includes six primary areas of responsibility:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

These apply to all merchants who accept payment cards. This includes merchants who accept cards only over the counter, merchants who accept cards only over the internet, and merchants who contract with a card processor to accept cards over the internet. The merchant’s bank ultimately determines if the merchant meets the standards based on literal compliance or “compensating controls<sup>11</sup>.”

---

<sup>11</sup> A “compensating control” is an activity or process designed to decrease risk of a negative occurrence that is utilized when the situation or resources will not allow implementation of a preferred internal control mechanism.



#### 5.4 ***Appendix D: National Electronic Commerce Coordinating Council (EC<sup>3</sup>)***

The National Electronic Commerce Coordinating Council (EC<sup>3</sup>) describes themselves as “an alliance of national state government associations dedicated to the advancement of electronic government within the states.” They have identified best practices to implement successful electronic government with the lowest degree of risk.

In their document *Risk Assessment Guidebook for E-Commerce/E-Government* they identify eight areas of focus:

1. Leadership/Governance
2. Privacy
3. Security
4. Technology
5. Legal Readiness
6. Customer Readiness and Accessibility
7. Applications
8. Competencies

The auditors used these best practices as guidelines as they related to the audit’s objectives.

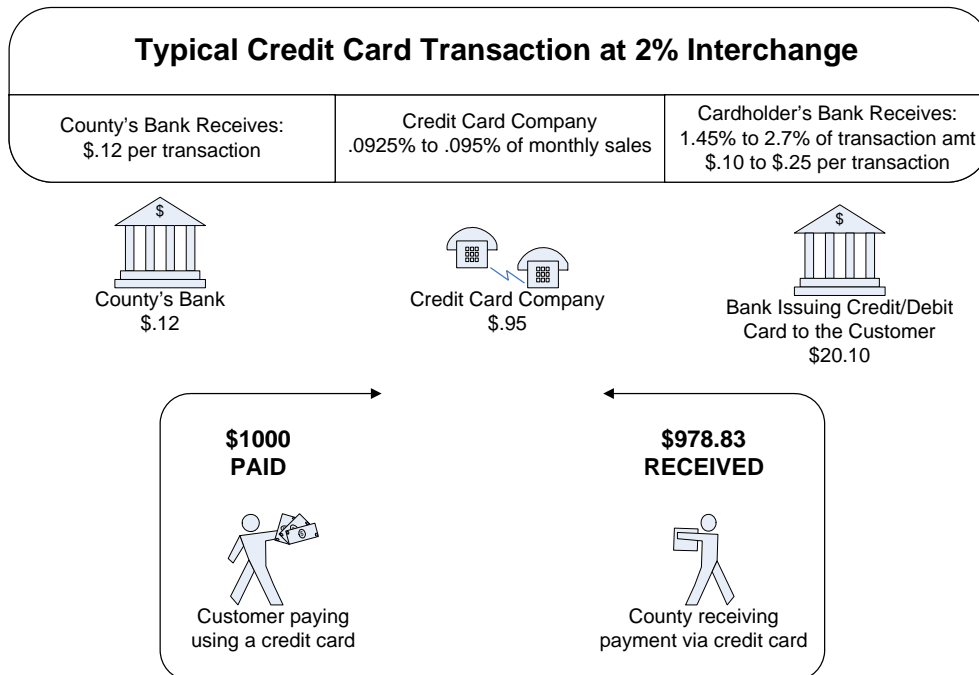


### 5.5 Appendix E: Interchange

The following description of “interchange” is excerpted from the 2006 Government Accountability Office (GAO) report, *Credit Cards: Increased Complexity in Rates and Fees Heightens Need for More Effective Disclosures to Consumers*.

When a consumer makes a purchase with a credit card, the merchant selling the goods does not receive the full purchase price. When the cardholder presents the credit card to make a purchase, the merchant transmits the cardholder’s account number and the amount of the transaction to the merchant’s bank. The merchant’s bank forwards this information to the card association, such as Visa or MasterCard, requesting authorization for the transaction. The card association forwards the authorization request to the bank that issued the card to the cardholder. The issuing bank then responds with its authorization or denial to the merchant’s bank and then to the merchant. After the transaction is approved, the issuing bank will send the purchase amount, less an interchange fee, to the merchant’s bank. The interchange fee is established by the card association. Before crediting the merchant’s account, the merchant’s bank will subtract a servicing fee. These transaction fees—called interchange fees—are commonly about 2 percent of the total purchase price.... In addition, the card association receives a transaction processing fee.

Figure 6



Source: Snohomish County Office of the County Performance Auditor



## 5.6 Appendix F: Per-Transaction Fees

All credit and debit cards are not the same. Although some cards are solely credit cards and a few are debit only, some payment cards may be processed multiple ways.

Figure 7

	<b>Credit</b>	<b>"Offline" Debit AKA "Check Card" AKA "Signature Debit"</b>	<b>"Online" Debit AKA "PIN Debit"</b>
<b>What is it?</b>	<p>*A card is swiped through a magnetic card reader</p> <p>*The customer signs a receipt if they are present</p>	<p>*A card is swiped through a magnetic card reader</p> <p>*The customer signs a receipt if they are present</p>	<p>*A card is swiped through a magnetic card reader</p> <p>*The customer keys their PIN code</p> <p>*Electronically authorized</p>
<b>What tools do you need?</b>	<p>*A magnetic card reader</p> <p>*A credit card or credit card information</p>	<p>*A magnetic card reader</p> <p>*A debit card or debit card information</p>	<p>*A magnetic card reader with PIN pad or a card reader with add-on PIN pad</p> <p>*In-person customer</p>
<b>What does it cost?</b>	<p>Analysis of County charges show a range of 1.43–2.95% plus \$.10 for each transaction</p> <p>Mode 1.43% + \$.10 for Visa</p> <p>Mode 2.05% + \$.10 for MC</p>	<p>Analysis of County charges show a range of 0.8–2.21% plus \$.25 for each transaction</p> <p>Mode of 0.80% + \$.25</p>	<p>PIN debit is a flat interchange fee of <b>\$.65</b> for each transaction</p>
<b>Notes:</b>		<p>*Lower interchange fees than credit for transactions above a certain dollar amount</p>	<p>*Reduced chargebacks</p> <p>*Lower interchange fees for most transactions</p>

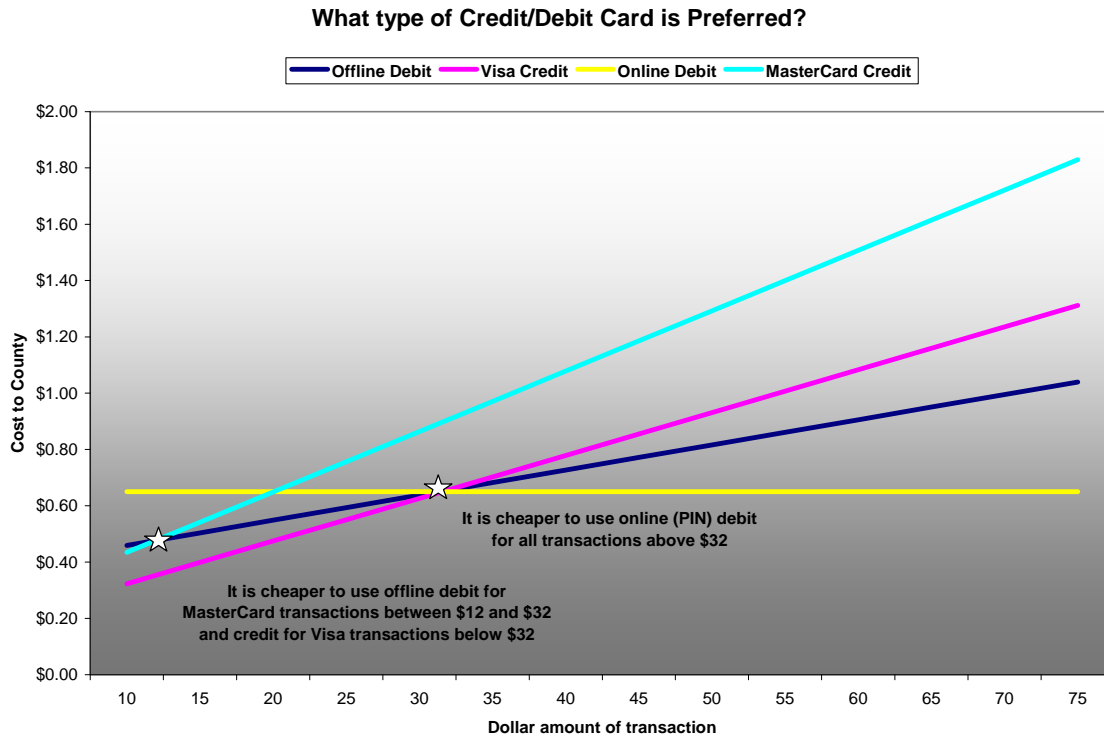
Source: Snohomish County Office of the County Performance Auditor



In analysis of types of payment cards, the auditors identified that different types of payment cards may be optimal for different transactions. The “Cost to the County” on the Y axis of Figure 8 is the combination of interchange and other fees the county would pay for a transaction at each dollar amount on the X axis using the four different types of payment cards.

If a transaction is above \$32, it is cheapest for the county to accept PIN debit cards. Transactions below \$12 are cheapest to process as credit. Between \$12 and \$32, it becomes more complicated. If the customer presents a Visa card, it is cheaper to process the card as credit; and if the customer presents a MasterCard, it is cheapest to process it as signature debit.

Figure 8



**Source:** Snohomish County Office of the County Performance Auditor

\* This chart is based on a set of cost assumptions. If bank fees, interchange rates, and/or other card fee structures change this data may no longer be valid.