Application Guide

Siebel Self-Service for Cards

Table of Contents

1

Overview

1.1 Introduction to Siebel Self-Service for Cards

Siebel Self-Service for Cards is the complete enterprise-class customer self-service and e-billing solution of Siebel, providing the out-of-the-box application necessary for delivery of sophisticated self-service applications for card issuers. The Foundation Application, Siebel Card Manager, shows how cardholders can view their accounts and statements online, make electronic payments using ACH or other payment accounts, request new cards and profile changes, and perform self-service using the Internet. Siebel Self-Service for Cards is available for deployment under a traditional enterprise license model or as a Siebel managed solution in our Tier 1 data center.

This guide describes the components and architecture of Siebel Self-Service for Cards and explains how it meets the complex requirements and return on investment (ROI) goals of the world's largest card issuers.

Siebel Customer Self-Service Solution

Customer Self-Service (CSS) gives customers direct control over the full range of account-related tasks, from finding information to executing transactions, all independent of the device used to engage with the provider. It empowers customers to perform functions that might otherwise go through a call center, traditional retail outlet, or other distribution channel. CSS combines electronic bill presentment and payment, service request management, personalization and application integration technologies to create an integrated, natural and preferred starting point for all customer service issues.

Contact centers provide the key to unlocking potential business benefits through self-service. Analyzing contact center statistics shows that the vast majority - often 60-90 percent - of customer service issues relate to a cardholder's account. For this reason, Siebel's product solutions provide direct access to detailed account information and interface with complementary front- and back-office systems to provide access to a variety of account-related services.

Siebel Self-Service for Cards is a packaged suite of applications specifically for the issuers, to enable service providers to fully realize the benefits of this new online self-service way of doing business. The number of card holders actively using online self-service and e-billing is steadily increasing. Livermore Research estimates that 100M of 360M US cardholders will be active enrolled users of issuers online service applications.

Siebel Self-Service for Cards includes a rich set of applications & functionality that give providers a complete multi-channel customer-self service experience. This suite includes product solutions for:

- e-Billing and Payment

- Account Service Requests

- Reporting and Cardholder Analytics

As a packaged solution, Siebel Self-Service for Cards is designed as a functionally complete application with a rich set of out-of-the-box capabilities. The look and feel of the application is fully configurable to the unique branding and customer flow of individual issuers.

Siebel Self-Service for Cards includes:
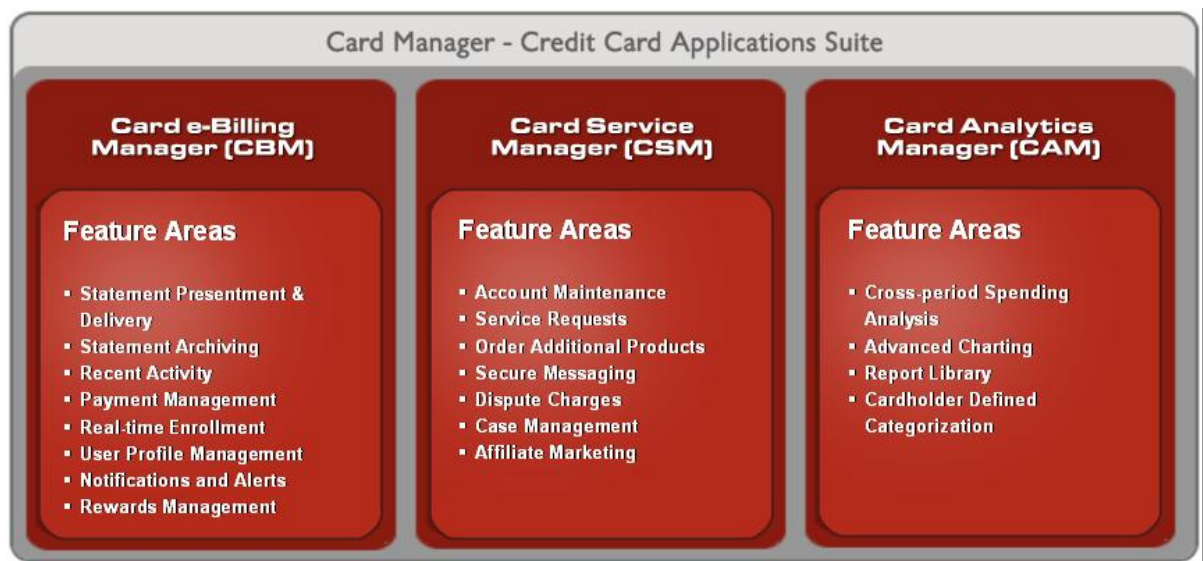
Business Benefits of Siebel Self-Service for Cards

By offering cardholders a compelling online experience to manage their accounts, issuers are able to maximize online adoption and usage of the low cost web service channel.

Issuers are able to achieve reduced customer service costs by:

- Deflecting and eliminating customer calls to live agents

- Decreasing paper, postage and lockbox payment processing costs

- Reducing fraud through increased account diligence and cardholder notifications

Improved customer satisfaction from the convenience of 24x7 access to account information increases cardholder retention, generates revenue from better online cross-sell capabilities and differentiates the service level provided to card portfolios.

As a production proven platform, Siebel Self-Service for Cards reduces infrastructure cost and provide the best cost of ownership for issuers. Siebel superior scalability reduces the hardware footprint and IT resource needs of alternative approaches.

Additional Modules Available

Siebel offers additional products to complement the Siebel Self-Service for Cards:

CSR Manager - The browser-based customer service application that reduces call management costs by providing critical account management access and capabilities to customer service representatives.

Email Response Management - An intelligent application that enables automated response and recommended response to email inquiries, improving agent productivity and customer satisfaction with faster responses.

Marketing Manager - The personalization and campaign management solution that enables organizations to increase revenue and decrease customer care costs by weaving personalized marketing and customer service messages throughout the Customer Self-Service experience based on actual account, profile or CDR data.

Syndication Manager - A cartridge-based content distribution system that gives organizations the ability to publish customers. summary account information to portals and aggregators. Syndication Manager provides customers with the convenience of All Portals Addressable access to account information.

IVR Manager- Delivers self-service account management capabilities via a fully integrated IVR communication channel.

Print Manager - Complements self-service and e-billing by offering an integrated data consolidation and print statement design solution for generating print statement output.

Intelligent Assistant (IA) - An advanced, Natural Language based search and self-service application, IA enables users to quickly find answers to both general content and personal account queries using everyday, conversational language.

EasyPay - A self-contained quick payment solution that allows customers to execute one-time/last minute payment transactions using the web, IVR or CSR without requiring the customer to formally enroll for online self-service.

1.2 Conceptual Overview
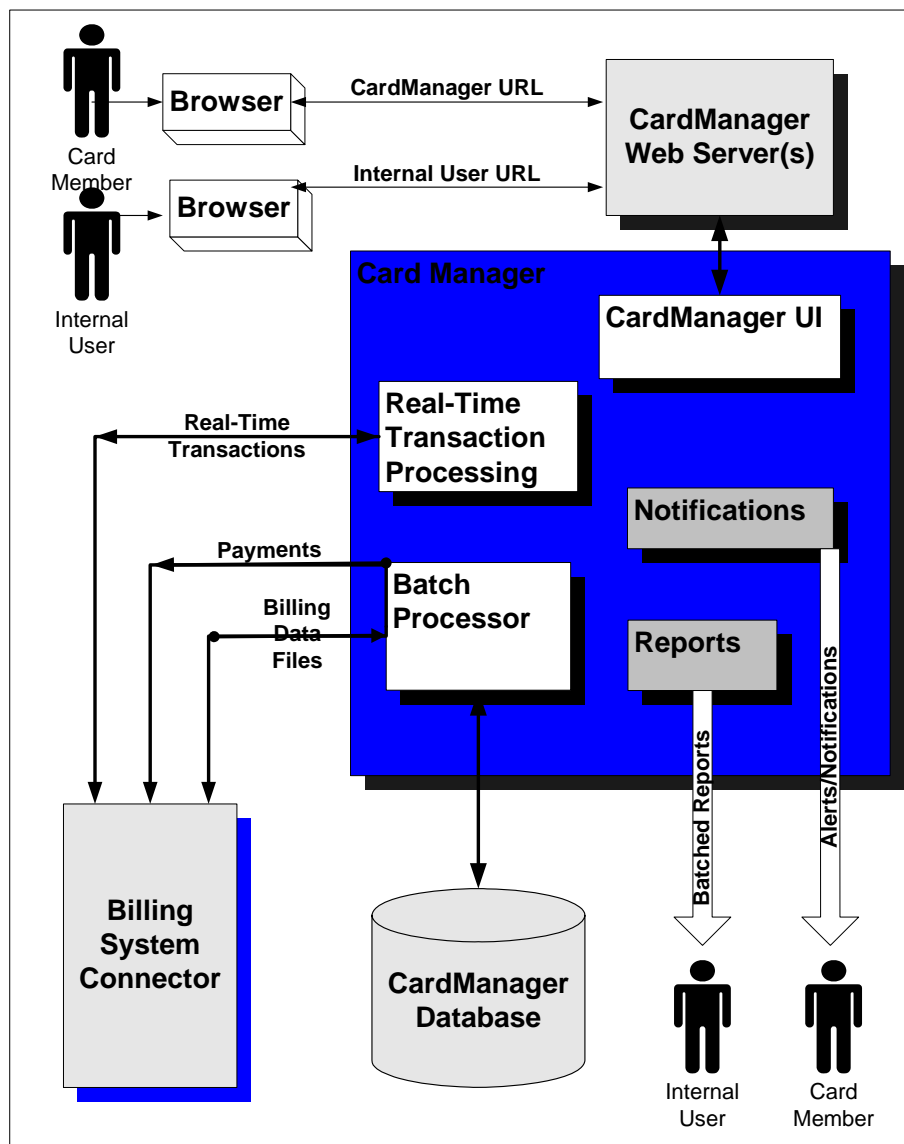
Figure 1.1 – System Context Diagram

Siebel Self-Service for Cards System Components

The Siebel Self-Service for Cards system consists of three key components:

♦ **Siebel Self-Service for Cards UI** – The user interface giving card members access to the core functions of the Siebel Self-Service for Cards system

♦ **Billing System (ODS) Real-Time Interface** – A real-time interface to the billing system for handling requests from Siebel Self-Service for Cards for real-time information from ODS using MQSeries messaging.

♦ **Billing Data File Batch File Delivery/Processing** – An interface for delivery of daily transaction data and monthly statement data processed by FDR.

Siebel Self-Service for Cards Application Back-End Components

Siebel Self-Service for Cards applications provide a number of separate back-end components, which are configured to deliver the required functionality:

♦ **Reporting** – Generates reports in response to online or scheduled requests for analytics data.

♦ **Alert Notifications** – Generate e-mail notifications. These are triggered by system events or data-driven batch processing events.

2

Siebel Self-Service for Cards Application Use Cases

2.1 Overview

The following set of use cases serves as the functional specification for the system. Each use case specifies a set of activities that can be performed by an actor (e.g., card member) to achieve a desired goal. It also describes the set of interactions between the actor and the Siebel Self-Service for Cards foundation application (called Card Manager).

In order to fulfill its goal, a use case may also interact with external systems, which are systems that are outside the boundary of the application, such as the billing system.

There may be many possible paths through a use case. The main path describes the successful completion of the use case without encountering any exceptional conditions. Alternate paths describe other related paths through the use case (for example, add, edit and delete) that are considered not to be a part of the common flow of the use-case. These are labeled using numbers in square brackets, e.g., [A1], Exception paths describe exception conditions and how they are handled. (e.g., [E1]). Business Rules are listed separately, where appropriate (e.g., [B1])

The use cases in this document describe the essential interaction between the actors and the Card Manager application. The User Interface (UI) consists of a set of screens and navigation elements with interfaces (APIs) to Siebel Self-Service for Cards platform functions, which provide access to statement and payment information. The card member presentation is driven by a set of HTML templates (Tiles). The navigation and control is driven through a standard Java framework (Struts).

The use cases in this document form the basis for functional test cases, defining how the screens, as well as the system as a whole, should function from a user perspective.

2.2 Actors

ACTOR	EXAMPLE ROLES	NOTES
Card Member	End User	The card member is the user of the Siebel Self-Service for Cards Application. Card Members perform following actions such as: enroll, login, view statement and transactions, make payments, request services, NLS, Secure Messages.
CSR User	Phone Rep (CSR) Phone Rep (Collector) Contributor Case Owner Info Security Rep Administrator Helpdesk Administrator Manager Executive Manager Case Reviewer Fraud Rep	Users will be assigned one role and will be given the privileges associated with this role
System	Siebel Self-Service for Cards Application	The system includes multiple components handling different functions such as enrollment, login, payment, administration, etc.
Operator	Administrator of Siebel Self-Service for Cards system	Operators configure and manage the Siebel Self-Service for Cards system but are not responsible for managing CSR Users.

Figure 2.1 –Actors

2.3 CSR User Roles & Privileges

EXAMPLE ROLE	PRIVILEGES	NOTES
CSR User	Jump To Page Login As Card Member Reset Card Member Password Reset After Enrollment or Login Failure Disable/Enable Access View Card Member Profile View Payment History Mark Case Reviewed View Reports View Case Accept, Return and Escalate Case Assign Case Add/Change/Delete User Reset CSR User Password View Roles Update Roles	A representative from Info Security assigns a role to an CSR User when the user is created. Each role has a set of privileges assigned to it. The system will be configured with an initial set of roles, but the Info Security Rep may create additional roles. Users will also be assigned to one or more categories (departments), which are independent of the role they have been assigned.
Phone Rep (CSR)	View Card Member Profile Page Disable/Enable Access Jump To Page Reset Card Member Password Reset After Enrollment or Login Failure View Payment History	Phone reps may only view card member information and payment history. They may not view or work on cases (secure messages)
Phone Rep (Collector)	View Card Member Profile Page View payment history	Collectors are phone reps with limited privileges. There are about 2000 of these
Contributor	View Card Member Profile Page Disable/Enable Access Jump To Page Reset Card Member Password Reset After Enrollment or Login Failure	Contributors are caseworkers. They view and respond to secure messages. In doing this they may also perform any actions that a phone rep can perform. In addition, they may work on cases for categories that they have been assigned to. They may reply to secure messages

EXAMPLE ROLE	PRIVILEGES	NOTES
	View Payment History Accept, Return and Escalate Case	that they have taken off the queue, and may also return them to the queue or escalate them to an escalated queue.
Case Owner	View Card Member Profile Page Disable/Enable Access Jump To Page Reset Card Member Password Reset After Enrollment or Login Failure View Payment History Accept, Return and Escalate Case Assign Case View Roles and Privileges	Case Owners are managers who manage a number of Contributors in handling one or more categories of cases. They may work on cases, escalated cases, or assign cases to members of their team. They may also view the roles and privileges of Contributors in categories of which they are a designated owner.
Info Security Rep	Add/Change/Delete User Reset CSR User Password Update Roles	Info Security Reps manage security. They may add or delete CSR Users, assign them roles and categories, and reset passwords
Administrator	Add/Update/Archive Templates	Administrator only manages templates
Helpdesk Administrator	View Roles Reset CSR User Password	Helpdesk Administrators may view roles and privileges, but the only action they can perform is to reset CSR User passwords. They will see only the Manage CSR Users tab.
Manager	View Roles	Managers may need to see individuals profile to see what privileges that they have but not make any changes
Executive Manager	View Roles Login As User	Executive Managers need access to all functions.
Case Reviewer	View Case	Case Reviewers may view any cases, but take no actions except to flag a case as having been viewed.
Fraud Rep	Enable/Disable Access View Reports	Fraud Reps will view fraud reports and may access the application to disable a card member.

Figure 2.2 – CSR Users Roles and Privileges

2.4 General UI

The following use cases detail common functionality that can be applied to more than one view in the Siebel Self-Service for Cards application.

Note: The UI needs to be handicap accessible.

2.4.1 Switch Language (200)

Name:	Switch Language
Brief Description:	System redisplays page in selected language
Trigger:	Card Member toggles language on current display
Main Path:	1. System updates the static content of the user interface 2. System updates the language indicator in card member's profile 3. Use case ends

2.4.2 Display Error Message (210)

Name:	Display Error Message
Brief Description:	System redisplays page with an error message
Trigger:	Card Member performs an action that cannot be completed
Main Path:	**1.** System determines required error actions **2.** System reads error message text from a configuration file **3.** System updates information on page as necessary **4.** System redisplays page with error message (displayed in Red) below heading and above first field **5.** Use case ends

2.4.3 Cancel (220)

Name:	Cancel
Brief Description:	Card Member selects a *Cancel* action

Main Path:	1. System returns card member to first page of current sequence of pages
	2. System clears any data or selections made by the card member
	3. Use case ends

2.4.4 Download Transactions (230)

Figure 2.3 – Download

Name:	Download Transaction Detail
Brief Description:	Card Member downloads the current view of transaction detail
Trigger:	Card Member selects download button
Main Path:	1. System opens a pop-up window:

<table>
<tr>
<td></td>
<td>

    a.   Data Types

         i.   Quicken (.qif)

         ii.   Money (.qif)

         iii. Comma Delimited (.csv)

         iv. Tab Delimited (.dat)

    b.   **Actions**: Download; Cancel

2. Card Member selects type of download from drop-down box and selects *Download*

3. Card Member's browser provides options for download

4. Card Member selects browser functions (Open, Save or Cancel) to complete download function

5. System closes pop-up window returning card member to the page that download was selected from

6. Use case ends.

</td>
</tr>
<tr>
<td>**Notes:**</td>
<td>

Uses standard browser download function.

Siebel Self-Service for Cards will download to Quicken and Money applications in QIF format but the drop-down menu will display four options: Quicken (.qif); Money (.qif); Comma Delimited (.csv); Tab Delimited (.dat).

</td>
</tr>
</table>

2.4.5 Page through data in a table (240)

Figure 2.4 – Paging Function

<table>
<tr>
<td>**Name:**</td>
<td>**Page through data within a single view**</td>
</tr>
<tr>
<td>**Brief Description:**</td>
<td>Card Member pages through large amounts of data that could appear on a single view</td>
</tr>
<tr>
<td>**Main Path:**</td>
<td>

1. Card Member selects single forward arrow to see the next page of data

2. Card Member selects double forward arrow to see the last page of data

3. Card Member selects single backward arrow to see the previous page of data

4. Card Member selects double backward arrow to see the first page of data

5. Use case ends.

</td>
</tr>
<tr>
<td>**Notes:**</td>
<td>

Page must display number of page and total number of pages, e.g., page 3 of 5

The number of lines displayed on each page is configurable and will be set initially to 20.

</td>
</tr>
</table>

2.4.6 Sort data in a table (250)

Name:	Sort data in a table
Brief Description:	Card Member sorts the data in a specific table
Main Path:	1. Card Member selects a sorting link (a column header that supports sorting) 2. System sorts the data in the table by the selected column in ascending order 3. Card Member selects the same sorting link 4. System sorts the data in the table by the selected column in descending order 5. Card Member selects a different sorting link 6. System sorts the data in the table in by the newly selected column in ascending order 7. Use case ends.
Notes:	If there are enough line items displayed to cause paging to be enabled, the sort will occur over all data, not just the data currently displayed on the page. All tables that display transactions will have ability to sort on column headings except for *Transactions* page, which cannot be sorted because it includes category sections and is therefore not sortable.

2.4.7 Display Brand (251)

Name:	Display Brand
Brief Description:	System displays brand graphic on every card member page
Main Path:	1. System determines correct graphic based on Card Code 2. System displays brand graphic on the page 3. Use case ends
Business Rules:	[B1] If the card type code is not found in the table provided by the customer, the system should not display any graphic image.
Notes:	Card Type Code mapping and corresponding graphics needs to be provided by the credit card issuer.

2.4.8 Attempt Access with Session Timed Out (252)

Name:	Attempt Access with Session Timed Out
Brief Description:	Card Member attempts to perform an action after the card member's session has expired.
Main Path:	1. System redirects user to an error page with a link to the Login Page

	and an error message asking the card member to login again
	2. Use case ends
Business Rules:	[B1] The session time is configurable and will be set initially to 15 minutes.
Notes:	The card member's session may expire while the card member is on any page.

2.4.9 Display Verified By Visa Graphic (253)

Name:	**Display Verified by Visa Graphic**
Brief Description:	For VISA applications the system will display the Verified By Visa graphic
Main Path:	**1.** System displays a graphic under the Quick Links which links to a Verified By Visa site (see notes below)
	2. Use case ends
Notes:	Visa regulations require for any website the site has to have the availability for a card member to sign up for their 'Verified by Visa' program. This allows the card member and merchant to transact on-line with a unique password. To support this, a logo needs to be added with links to URLs behind it.
	The graphic is:
	Card Type Code mapping to VISA accounts needs to be provided by the credit card issuer.
	Else do not display the Verified By Visa graphic

2.5 Enrollment Use Cases

The Enrollment use cases cover the business requirements for allowing card members to enroll and use the system.

This section consists of the following use case:

- **Enroll** – Card member provides a username and password to access the system

2.5.1 Enroll (100)

Figure 2.5 – Card Member Enrollment

Figure 2.6 – Card Member Enrollment Continued

Figure 2.6.1 – Card Member Enrollment Success
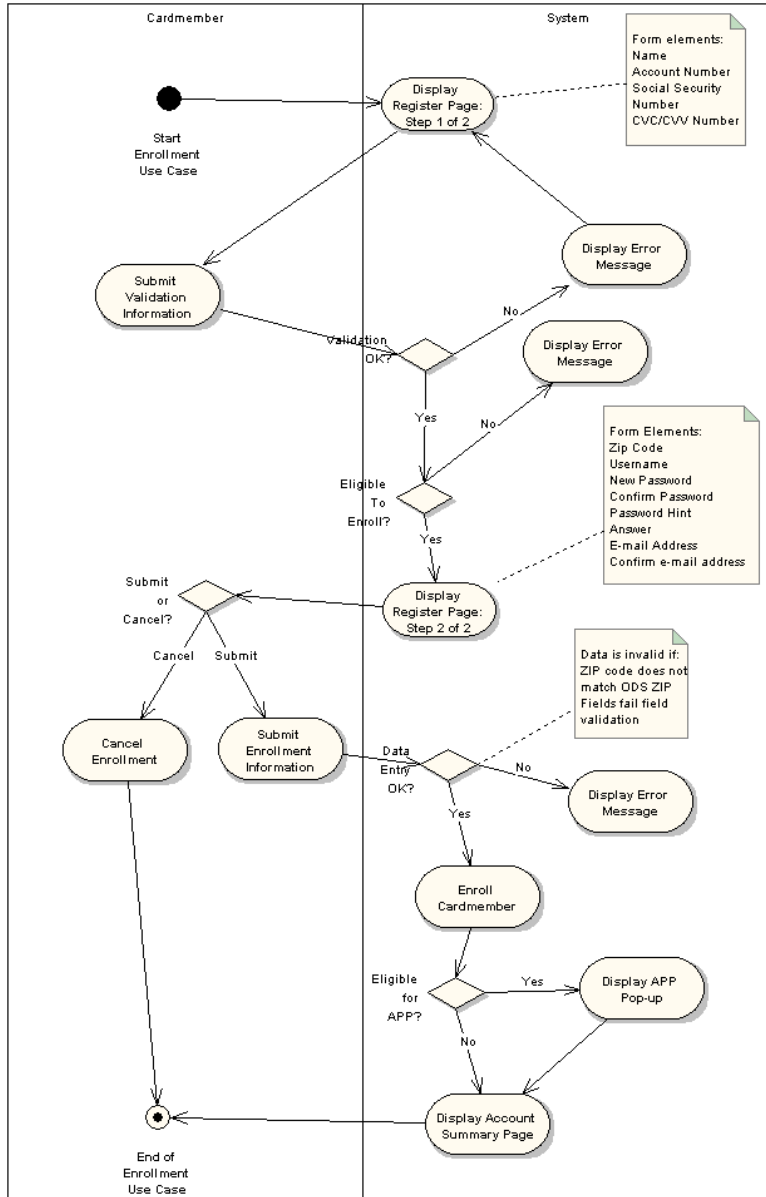
Figure 2.7 – Card Member Enrollment Activity

Name:	Enroll
Brief Description:	Card Member enrolls for the system.
Main Path:	1. Card Member clicks the Enrollment link
	2. System displays page 1 *Enrollment Page* containing the following form fields:
	a. Name (as it appears on credit card)
	b. Account Number
	c. Social Security Number
	d. Signature Panel Code (CVV/CVC)

e. **Actions**: Next; Cancel

3. Card Member completes the form and clicks *Next*

4. System checks that Account number is not already enrolled [E1] [E9]

5. System invokes **Read and Store Card Member Account and Status Information** use case [E2]

6. System invokes **Validate CVV/CVC Number** use case

7. System validates that enrollment information entered by card member matches data returned from the billing system: Name, Soc Sec; CVV and Account number [E3] [E4]

8. System validates that card member is eligible for enrollment [B2] [E5]

9. System displays enrollment page 2:
   a. Billing Zip Code
   b. Username
   c. New Password
   d. Confirm Password
   e. Secret Question, e.g. Mother's maiden name
   f. Answer
   g. E-mail Address
   h. Confirm e-mail address
   i. Agree to terms checkbox
   j. **Actions**: Submit; Cancel

10. Card Member selects Agree to Terms checkbox

11. Card Member selects *Register* [E9]

12. System validates fields entered by card member [E6] [E7] [E8]

13. System creates a enrollment record in the database

14. System sends ODS request to update e-mail address

15. System sends ODS request to the billing system to flag the card member as enrolled in billing system database

16. System **sends an enrollment welcome e-mail** to the e-mail address on record

17. System displays enrollment page 3 *New User Registration confirmation* page
    a. **Actions**: Access Your Account

18. Card Member selects *Access Your Account* action

19. System redirects card member to *Account Summary* page [A1]

20. Use case ends

Alternate Paths:	**[A1] Card Member selects Cancel:**
	1. System redirects card member to the *Login* page
Exception Paths:	**[E1] Account is already enrolled: [B1]**
	1. System displays message that the card member is unable to enroll
	[E2] Card Member enters Account number that doesn't exist at billing system:

	1. System redisplays page with a generic message saying that one or more fields are invalid
	a. Card Member enters value in one or more of CVV, SSN that doesn't match value returned from the billing system or Name is invalid AND one of the other fields is invalid:
	2. System redisplays page with a generic message saying that one or more fields are invalid
	3. System increments failed count and stores fail reason
	[E3] Card Member is not eligible to Enroll [B2]:
	1. System displays new page same as Enrollment page but with no fields and a specific error message page saying that the card member may not enroll
	[E4] Billing Zip Code does not match ZIP code returned by the billing system:
	1. System redisplays the page with a specific message saying that the Billing Zip Code is invalid
	2. System increments fail count and stores fail reason
	[E5] Card Member enters invalid User Name, Password, Secret Answers, E-mail Address, or does not check accept Terms and Conditions box:
	1. System redisplays the page with a specific message
	[E6] Password and Confirm Password don't match:
	1. System clears field and displays message stating that the passwords do not match
	[E7] Card Member fails to enroll after 3 attempts: [B3]
	1. System locks account number so that it cannot be enrolled
	2. System logs the unsuccessful enrollment attempt with date/time, values of account number, CVV, SSN, Billing Zip, lockout reason in database
	3. System displays a generic message and refers card member to Customer Service
	[E8] Card Member attempts to enroll and is Disabled
	1. System displays new page same as Enroll page but with no fields and a generic error message page saying that the card member account is not available and the card member should call Customer Service for more information
Business Rules:	**[B1]** Check for account enrollment already in Siebel Self-Service for Cards database. If present, do not allow re-enrollment.
	[B2] If ODS External Status Code is A, B, L, U, Z, F, I, or if External Status Code is C with current balance zero or negative, the system displays new page same as Enroll page but with no fields and a specific error message page saying that the card member may not enroll.
	[B3] If card member enters a valid Account number and fails 3 times to enroll, the account will be locked out and the CSR User will have to unlock the account before it can be enrolled. The system will store the lockout reason and fields that didn't validate in database, display a "generic message" to the card member.
	[B4] CSR Users are enrolled as users of the system in the same way as card members, but the system will not allow them to use card member functions. Also, the CSR User may enroll separately with

	the same User Name in the card member application.
Notes:	Mask password with asterisk
	Auto-tab between field entries, e.g. after three digits are entered for first segment SSN, the cursor will skip to the next field
	All calls are validated using primary card member account number
	System will display a picture of how to use the CVV on first enrollment page. (See TicketMaster for example)
	Expiration date corresponding to the CVV may have changed from what is on the card, so system should call ODS to get CVV with current expiration date, if it fails do it with reissued expiration date, if that fails do with manually updated expiration date.
	Any time Siebel Self-Service for Cards application presents a generic authentication error message, it needs to capture the reason for failure in database for management reports.
	System forwards E-mail to the SMTP server using the e-mail address on record and does not do any further validation of the e-mail address or handle returned e-mails. All e-mail will have a return address that has the bank's domain name and will be handled by an e-mail server at the bank. The bank will handle all bounced e-mails and reporting on returned e-mails.
	Default Bank Name (nickname) will be set for first time users (e.g., My Bank) so user doesn't need to enter anything when logging in for the first time.
	When customer enrolls the system sends on ODS request to the billing system to set card member to enrolled status (sets Misc 8_5 field in CHDHLDR view to "R")
	Secret questions drop-down will have 11 choices:
	1. What city were you born in?
	2. What is your Father's middle name?
	3. What is your Mother's middle name?
	4. What was your first job?
	5. What was your high school mascot?
	6. What is my favorite food?
	7. What is my favorite sports team?
	8. Who was my childhood hero?
	9. What is my favorite beverage?
	10. What is my favorite hobby?
	11. Who is my favorite author?
	Once enrolled, a card member may not un-enroll or re-enroll, but may Disable the online account by calling an CSR User
	If the card member selects Cancel from either Step 1 or Step 2 of New User Registration, the system will redirect them to the Login page.
	1. The card member is required to check the "I Agree" box and then submit. If they check Submit and do not check "I Agree" they receive error message stating they must check this to enroll.

Form Validation

NAME	DESCRIPTION	VALIDATION
*Billing Zip	Billing Zip Code	Numeric. Has to be 5 digits. ZIP code must match (first 5 digits of) billing system ZIP code
* Name	Name of card member as it appears on the Card	Alphanumeric. Max. length = 26 Name should match billing system name after stripping out spaces and other special characters. Not case sensitive.
*Card Account Number	Account number of card being enrolled.	Numeric. Max. length = 16
*SSN	SSN of card member	Numeric. Max. length = 9
*E-mail address	E-mail address of card member	Max. length = 50 Standard e-mail validation
*CVC/CVV #	3 digit # that appears on card	Numeric. Max. length = 3
*Username	Created by card member	8-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive. Must be unique in the system.
*Password	Created by card member. Display is masked using asterisks	6-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive. Can't be same as User name or answer to secret question
*Confirm Password		Must be same as password
*Answer	card member enters text in response to first password hint (secret question) selected from a pull-down list	Can't be same as password or User name

* – Field is required

2.6 Login Use Cases
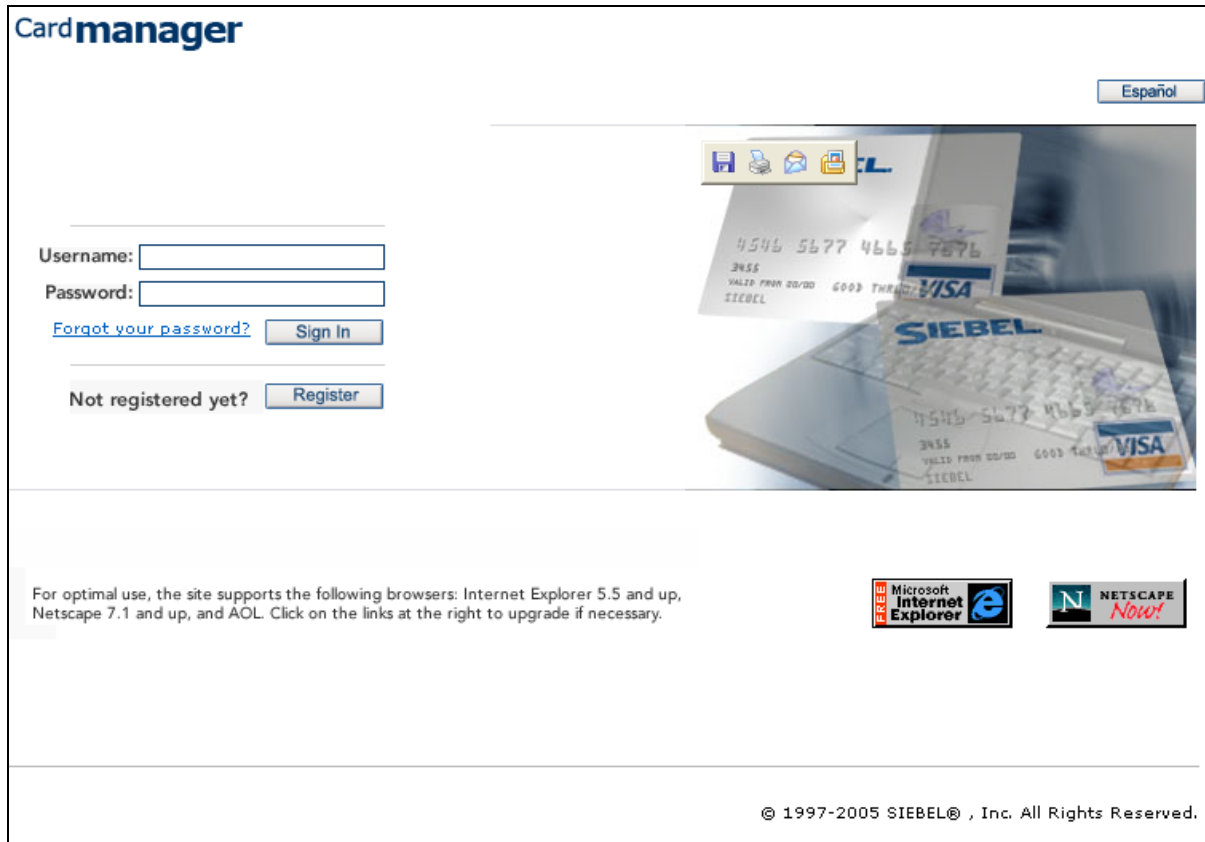
The login use cases cover the business requirements for allowing card members to authenticate and access the system. These card member level use cases specify the functionality required to satisfy these requirements in such a way that Siebel Self-Service for Cards can be configured, queries defined, screens developed, and any custom code developed to fulfill the use cases.

This section consists of the following use cases.

- **Log In** – Card member provides a username and password to access the system

- **Forget Password** – Card member forgets password and is presented a password reminder

- **Reset Password** – Card member resets an expired password

- **Log Out** – card member logs out

## 2.6.1 Log In (110)
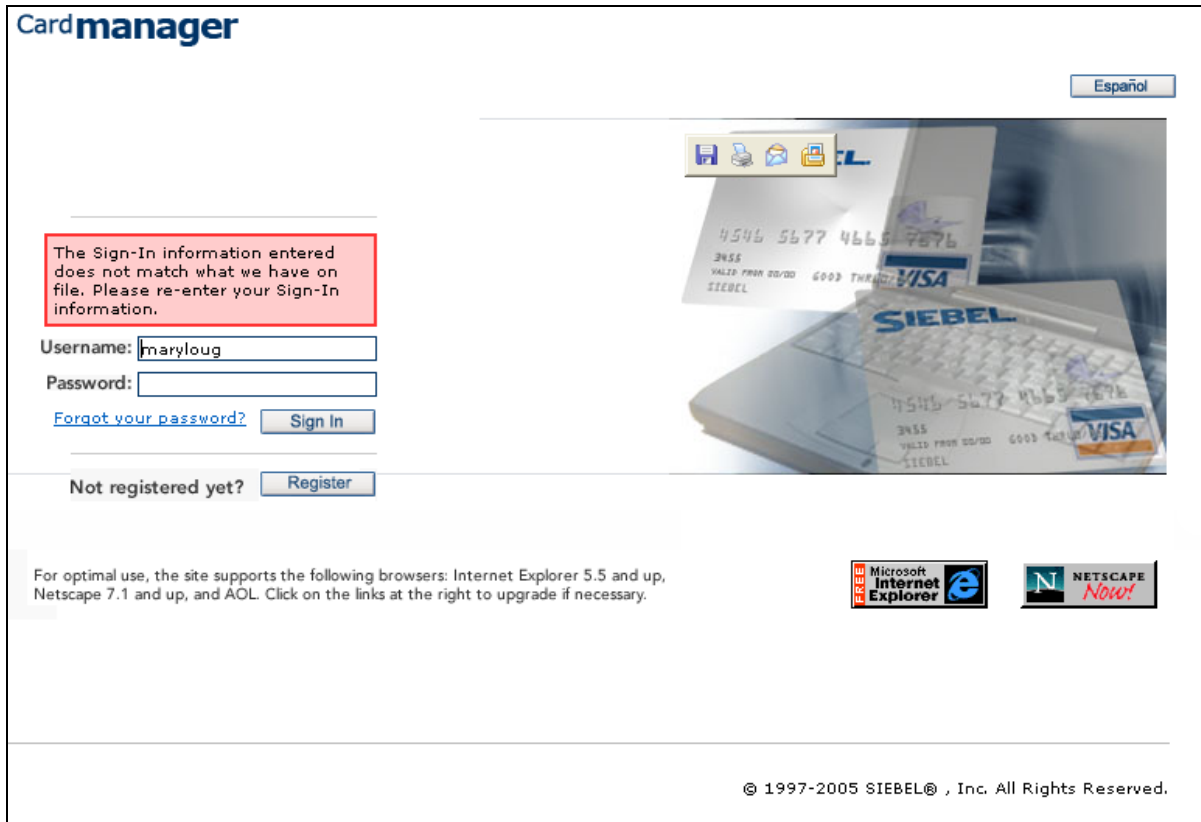
*Figure 2.8 – Login*

Figure 2.3 – Login Error
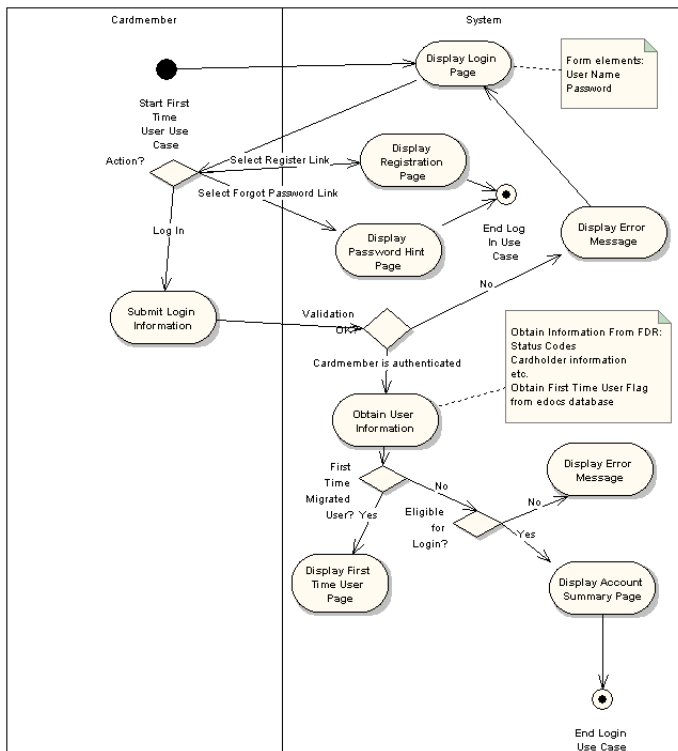

Figure 2.10 – Login Activity
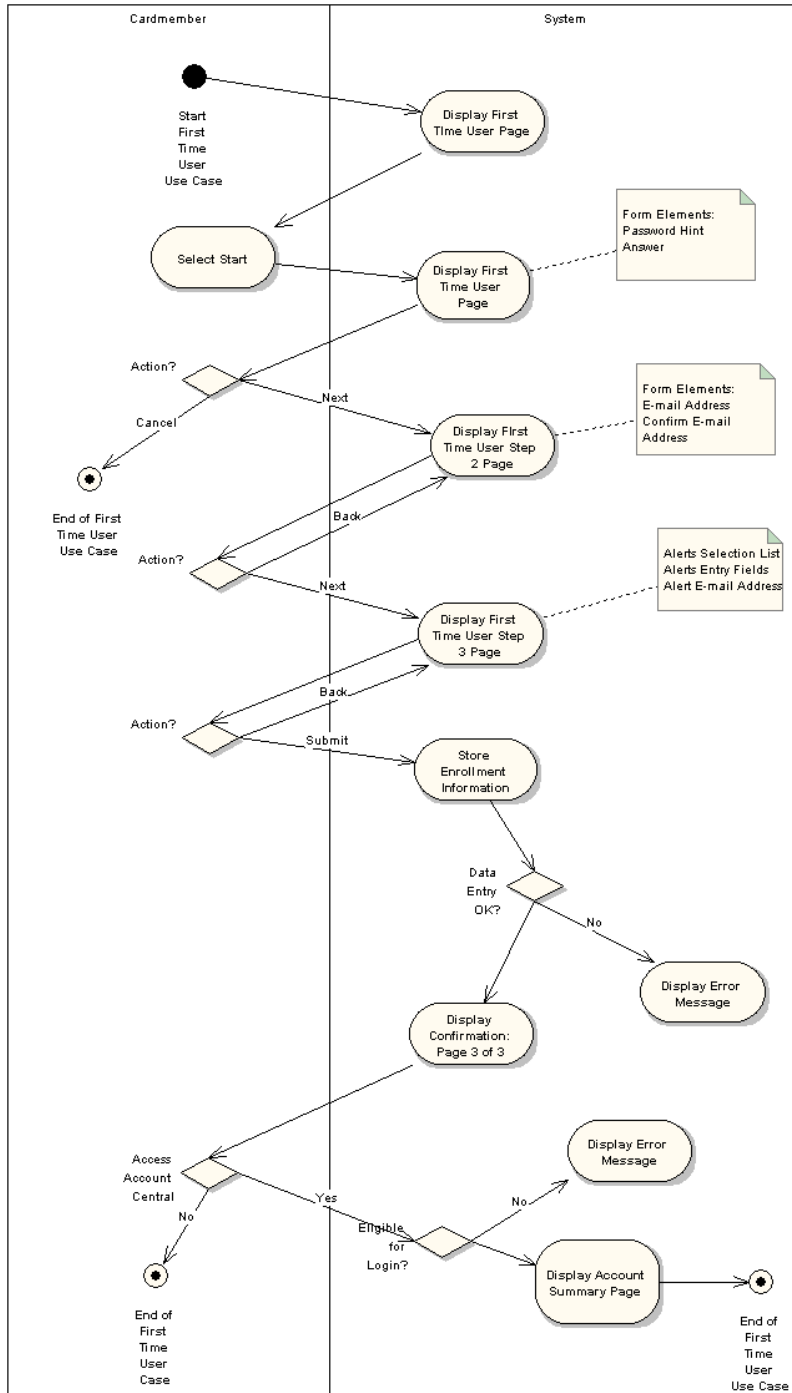
Figure 2.11 – Login First Time User

The Login User and Login First Time User activity diagrams shows the main activity flow for the *Log In* use case. It does not show every alternate path and is not intended as a detailed description of the use case.

Name:	Log In
Brief Description:	Card Member supplies a username and password to access the system.
Main Path:	1.　Card Member selects a link to login to the system 2.　System presents a form containing the following: 　　a.　Username 　　b.　Password 　　c.　**Actions**: Forgot Password; Sign In; Register 3.　Card Member completes the form and logs in [A1] [A2] 4.　System authenticates card member and gets card member's account number 5.　System invokes **Read and Store Card Member Account and Status Information** use case [E1] 6.　System checks that card member is allowed to log in [B1] [E2] 7.　System forwards card member to *Account Summary* page [A4] 8.　Use case ends
Alternate Path:	**[A1] Card Member enters incorrect username or password** 　　1.　System displays the Login Error page 　　2.　Use case continues from step 3 **[A2] Card Member was previously locked out and logs in with a temporary password [B2]:** 　　1.　Invoke **Reset Password** use case 　　2.　Use case continues from Step 2 of main path
Business Rules:	**[B1]**　If ODS External Status Code is A, B, L, U, Z, F, I, or if External Status Code is C with current balance zero or negative, the system displays new page same as Login page but with no fields and a specific error message page saying that the card member may not login **[B2]**　If card member password has been reset by an CSR User, the system sends card member a temporary password by email and system prompts the user to change the temporary password the next time card member logs in. **[B3]**　APP eligibility: IF Language is Spanish OR External Status is Z, B, L, U, E, F, I OR C with a current balance of 0 or less OR Internal Status is D, O, X OR Portfolio (PORTFOLIO_FLG of CHDHLDR View) is 18, 19, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 43, 44 OR Insurance Status Code (INSR_STTS_CD on CREDIT_LIFE_INSURANCE view) is F, R, D THEN card member is ineligible for APP
Exception Paths:	**[E1]　Card Member information could not be retrieved from the billing system:** 　　1.　System redisplays page with a generic message saying system is unavailable

[E2]   Card Member not eligible to log in [B1]

1.   System displays new page same as Login page but with no fields and a specific error message page saying that the card member may not login

[E3]   Card Member attempts to login and has an existing session

1.   System displays new page same as Login page but with no fields and a specific error message page saying that the card member may not login

[E4]   Card Member attempts to login and is locked out

1.   System displays new page same as Login page but with no fields and a specific error message page saying that the card member is locked out and must call Customer Service

[E5]   Card Member attempts to login and is Disabled

1.   System displays new page same as Login page but with no fields and a generic error message page saying that the card member account is not available and the Card Member should call Customer Service for more information

Notes:	The system needs to store information from ODS calls in the card member session for future use in navigation. System should store the following in session:

1.   For APP: from CHDHLDR view get External Status Codes, Internal Status Codes, Portfolio Flag. From CREDIT_LIFE_INSURANCE view, get Insurance Status Codes. The Insurance Status Code should only be checked if the card member passes all the other exclusion criteria.

2.   For Direct Bill Pay: from CARDHOLDER_NAME get number of plastics.

3.   For Paper Suppression: Eligibility code (Misc_Field_10 Pos 6) value E = eligible, Paper status code (value W=OFF)

4.   For Account Summary: Profile fields from CHDHLDR view

CSR User needs to know which card members are active, so at any one time, the card member should only be allowed one session.

The system will track the source of the login by obtaining a code from the URL at login. This code will be used to track effectiveness of promotions on a tracking report that identifies the pages visited by card members with different tracking codes. (Defer to 5.2)

If an CSR User is impersonating the user and the user is a "first-time user," then the CSR User will be taken directly to Account Overview screen, by-passing normal card member enrollment steps. The card member will then need to enroll as first-time user when he/she first logs in.

Field Validation

| NAME	DESCRIPTION	VALIDATION
*Username	Look up in Siebel Self-Service for Cards database	8-12 alphanumeric. Not case sensitive. Must exist.
*Password	Display is masked using asterisks	6-12 alphanumeric. Not case sensitive. Must match value stored in the Siebel Self-Service for Cards

2.6.2 Forget Password (120)

**Figure 2.12 – Card Member Forgot Password – Step 1**

**Figure 2.13 – Forgot Password - Step 2**

Figure 2.14 – Forgot Password - Step 3
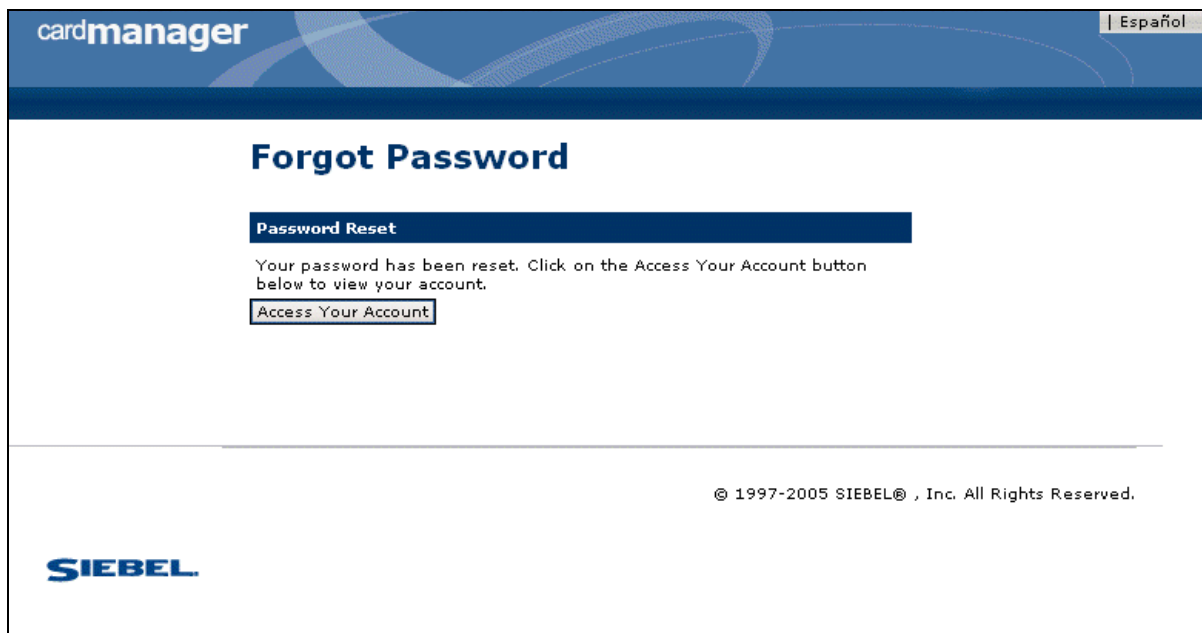
Figure 2.15 – Forgot Password - Success

Name:	Forget Password
Brief Description:	Card Member forgets password and systems presents a password reminder.

Main Path:	1. Card Member selects "Forgot Password?"
	2. System displays *Forgot Password Step 1* page containing
	a. Login ID
	b. Social Security Number
	c. **Actions:** Next; Cancel
	3. Card Member completes form and clicks *Next*
	4. System validates SSN [E2]
	5. System invokes **Read and Store Card Member Account and Status Information** use case [E1]
	6. Systems displays *Forgot Password Step 2* page containing:
	a. Secret Question
	b. **Actions:** Next; Cancel
	7. Card Member answer question and clicks *Next*.
	8. System validates the answer to Secret Question [E2]
	9. Systems displays *Forgot Password Step 3* page containing:
	a. New Password
	b. Confirm New Password
	c. **Actions:** Next; Cancel
	10. Systems displays *Forgot Password Step 4 confirmation* page containing:
	a. **Actions:** Access Your Account
	11. Card Member selects *Access Your Account* action
	12. System forwards card member to *Account Summary* page
	13. Use case ends
Exception Paths:	**[E1] Card Member information could not be retrieved from the billing system due to invalid Login ID:**
	1. System redisplays page and displays error message
	[E2] Card Member enters invalid SSN:
	1. System updates invalid login count and logs reason for failure
	2. System displays Forgot Password Page 1 with a generic error message
	[E3] Card Member enters invalid answer to Secret Question:
	1. System updates invalid login count and logs reason for failure
	1. System displays Forgot Password Page 2 with a generic error message
Alternative Paths:	**[A1] Card Member does not correctly answer the secret questions after *3* attempts.**
	1. Card Member is locked out of system.
Notes:	System update count of login attempts for each incorrectly answered secret question and logs the attempt. The attempts will be reported on the fraud report.
	Path [A1] is a requirement but has been deferred until Release 5.2.

Form Validation

NAME	DESCRIPTION	VALIDATION
*Username	Look up in database	8-12 alphanumeric. Not case sensitive. Must exist.
*SSN	SSN of card member	Numeric. Max length = 9
*Answer	Card Member enters text in response to first password hint (secret question) selected from a pull-down list (See Enroll use case, Note 14)	Matches previously stored value

*** – Field is required**

2.6.3 Reset Password (130)

Figure 2.16 – Reset Password

Name:	Reset Password
Brief Description:	Card Member resets password.

Trigger:	Card Member logs in with a temporary password.

Main Path:	1. System displays Reset Password page containing the following fields:
	   a. Current Password
	   b. New Password
	   c. Confirm New Password
	   d. **Actions**: Submit; Cancel
	2. Card Member completes the form and submits
	3. System validates Current and New Password [A1, A2]
	4. System updates the password
	5. System resets the login failure count
	6. Use case ends

Alternative Paths:	**[A1] Card Member enters incorrect password**
	   1. System displays Reset Password Error page
	[A2] New password is invalid or does not match confirm password:
	   1. System clears page and displays a specific error message that the new password is invalid

Form Validation

NAME	DESCRIPTION	VALIDATION
*New Password	Created by card member. Display is masked using asterisks	6-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive. New password must not match username or answer to secret question
*Confirm Password		Must be same as password

* – Field is required

2.6.4 Logout (140)

Figure 2.17 – Card Member Logout

Name:	Logout
Brief Description:	Card Member logs out of system
Main Path:	1. Card Member selects the "Logout" link. 2. System invalidates session 3. System displays the Sign Out page a. **Action:** Sign In 4. Use case ends
Business Rules:	
Note:	The system will also invalidate the session after a timeout period. The session will be configured initially to timeout after 15 minutes.

2.7 Account Summary

The Account Summary use cases cover the business requirements that allow a card member to view a snapshot of the current status of their account.

This section consists of the following use cases.

- **View Account Summary** – Card member views account status and pays off their current charges

- **Account Summary Data** – Describes the account data shown.

2.7.1 View Account Summary (300)

Figure 2.18 – Account Summary

Name:	View Account Summary
Brief Description:	Card Member views a snapshot of current status and pays their current charges

Main Path:	1. Card Member successfully logs in to the system or selects *Account Summary*
	
	2. System checks if there are any important messages to display [B1]
	
	3. Systems displays *Account Summary* page including: [B2] [A1]
	    a. Account Summary module
	    b. Account Important Messages module
	    c. Natural Language Search module (optional module shown for reference only)
	    d. Secure Message module (Message Center)
	    e. The following graphs:
	        1. Category Breakdown of spending habits for past month
	        2. Credit Card usage over the previous 4 months
	    f. **Actions**: Manage Profile; Case Number; Pay Now; View Statement; Answer (optional)
	
	4. Use case ends

Alternate Paths:	e

Business Rules	**[B1]** If internal status code is D, O, X, there are Intuitive messages (important account messages). See Section 11.12, Intuitive Message Logic. The system will display these above Account Summary. The messages displayed are (in the order they should appear on the page):
	
	    1. If Internal Status Code = X: "Your Account is currently past due and over its assigned credit limit":
	
	    2. If Internal Status Code = D: "Your Account is currently past due"
	
	    3. If Internal Status Code = O: "You are currently over your credit limit"
	
	    4. If Payment Due Date – Today's Date < 10 AND Minimum Payment Due >0 AND NOT (Internal Status Code = D OR X OR O): Your payment is due in X days" (See table below, Account Summary Data, of values obtained by calling ODS).
	
	    5. If new statement is loaded into Siebel Self-Service for Cards database AND card member has not viewed it: "Your most recent statement is now available". Note: only one instance of this message should be displayed even if card member has not viewed previous month's statements.
	
	If there is no account history then the images are not displayed. If the chart data is not available chart will be suppressed
	
	For card members who are newly enrolled, there will be no Secure Messages so this module will not appear
	
	[B2] System will map the billing system MCC codes to the 16 customized Merchant Category Group Codes defined by customer
	
	[B3] If payment has been made during the billing cycle, the system will display "No Payment Due" instead of Payment Due Date. (determined by checking if STMT_MIN_PAY in CHDHDLR view is zero)

Notes:	The system will not display modules if there is no data.

<table>
<tr><td></td><td>Account summary data is obtained from the billing system (See table below). This is so that the data is as current as possible. Consequently, it is possible that some values will not be the same as transaction data obtained from nightly feeds.

E-mail address on this page should be populated from the card member's Profile. Updates will be provided to Siebel Self-Service for Cards in the Change Data file if the e-mail address is changed at system of record.

The Intuitive Messages contain links that will link to the *Make A Payment* page for payment due messages and to *Statements* page for Statement Available message

If a payment has been made during the billing cycle the billing system sets STMT_MIN_PAY in CHDHDLR view to zero</td></tr>
</table>

2.7.2 Account Summary Data

SIEBEL SELF-SERVICE FOR CARDS	ODS VIEW	ODS FIELD NAME	CAPTION
Payment Due Date	CHDHDLR	Payment Due Date	STMT_PAY_DUE_DATE
Minimum Payment Due	CHDHDLR	Minimum Payment Amount	STMT_MIN_PAY
Past Due Amount	CHDHDLR	Delinquent Amount	DELQ_AMT
Amount Over Credit Limit	CHDHDLR	Condition: Available Credit - if Available Credit is negative, display as a positive to indicate the overlimit amount	ATV_AVAL_CRD
Last Payment Amount	CHDHDLR	Last Payment, Amount	NM_AMT_LAST_PAY
Last Payment Credited On	CHDHDLR	Last Payment, Date	NM_DAT_LST_PAY
Total Credit Line	CHDHDLR	Credit Limit	ATV_CRD_LMT
Current Account Balance	CHDHDLR	Current Balance	ATV_CUR_BAL
Recent Activity (total authorizations outstanding)	CHDHDLR	**Formula:** Credit Limit **minus** Current Balance **minus** Amount Over Available Credit	ATV_CRD_LMT **minus** ATV_CUR_BAL **minus** ATV_AVAL_CRD
Total Credit Line	CHDHDLR	Credit Limit	ATV_CRD_LMT

Figure 2.19 – Account Summary ODS Field Data

2.8 Statement Use Cases

The statement use cases cover the business requirements that allow a card member to view current and historical statements, the ability to download the statement detail and produce a printer friendly page.

This section consists of the following use case:

- **View Statement** – Allow the card member to select and view a current or previous statement

2.8.1 View Statement (310)

cardmanager

Contact Us | FAQs | Sign Out | Español

My Account | Payments | Self Service | Help

View Account Summary | View Statements | View Recent Transactions | View Reports | Create Reports | Search Transactions

Quick Links

- ▶ Make a Payment
- ▶ View Statements
- ▶ View Recent Transactions
- ▶ Manage Profile
- ▶ Ask Us a Question
- ▶ Sign Out

SIEBEL

Statement

Garner Mary Loug
mnambiar@edocs.com
xxxx xxxx xxxx 5838
Last Login: 02/03/2005 2:54 PM EST

Statement Summary   Statement Closing Date 07/01/04 ▾ Submit

Payment Information		Account Summary		
New Balance	$285.08	Previous Balance		$797.79
Minimum Payment Due	N/A	Purchases	+	$130.05
Amount Past Due	$0.00	Cash Advances	+	$0.00
Payment Due Date	07/24/2004	Credits	-	$0.00
Total Credit Line	$6,400.00	Payments	-	$538.19
Total Available Credit	$0.00	Other	+	$0.00
Cash Advance Credit Limit	$3,200.00	Finance Charge	+	$0.00
Cash Advance Available Credit*	$0.00	New Balance	=	$285.08
Overlimit Amount	$0.00			

* Cash Advance Credit Limit is a Portion of Your Total Credit Line

View your list of transactions. Click the linked merchant/purchase description to edit the category or the memo.

Transactions

Printable Version | Download | Disclosure   Group By Category

Trans Date	Date Posted	Merchant/Transaction Description	Memo	Category	Amount
Purchases, Cash Advances & Fees					
02/19/04	02/19/04	BU SHOE DEPT 395 WALDORF MD		Auto Related	$50.00
02/19/04	02/19/04	BIG O TIRES #57 LOS GATOS CA		Auto Related	$100.00
02/19/04	02/19/04	DOLPHIN PET VILLAGE CAMPBELL CA		Clothing	$20.00
02/19/04	02/19/04	TARGET 00013086 FRAMINGHAM MA		Dining Out	$100.00
02/19/04	02/19/04	GSM WIRELESS SAN JOES CA		Health Care	$20.00
02/19/04	02/19/04	THE HOME DEPOT 3306 LAS VEGAS NV		Home Repair	$21.00
02/19/04	02/19/04	2CO.COM*DIETPROGRAM 877-294-0273 OH		Household	$10.00
02/19/04	02/19/04	KROGER #741 SL9 MADISON IN		Legal Services	$32.00
02/19/04	02/19/04	BIG 5 SPORTING #94 TORRANCE CA		Leisure	$63.00
02/19/04	02/19/04	TIAS TEX MEX' #6119 ARLINGTON TX D	📄	Misc	$30.00
02/19/04	02/19/04	EF INSTITUTE FOR CULTURL 8006655364 MA		Travel	$48.00
02/19/04	02/19/04	5165651133 AUTOPAYLANG*!01		Payments	-$100.00
02/19/04	02/19/04	CROSS SOUND FRRY SRVCS 860-443-7394 CT		Legal Services	$50.00
02/19/04	02/19/04	ENDODONTIC SPECIALISTS SHEBOYGAN WI		Health Care	$56.00
02/19/04	02/19/04	EDS/WALGREEN'S BOSTON, MA D		Financial	$47.00
02/19/04	02/19/04	OXT*1307911240 0204 800-950-7732 MI		Computer Related	$258.00
06/18/04	06/18/04	CHEVRON #00093357 MALIBU CA D		Home Repair	$15.01
06/22/04	06/22/04	SEARS ROEBUCK 2338 REDDING CA D		Utilities	$100.49
07/01/04	07/01/04	LATE FEE			$100.00
Total					**$1,020.50**
Payments & Credits					
06/02/04	06/02/04	PAYMENT - THANK YOU		Payments	-$338.19
06/13/04	06/13/04	PAYMENT - THANK YOU	📄	Legal Services	-$200.00
06/16/04	06/16/04	CAL STEAM-MARIN 4154592009 CA	📄	Utilities	-$105.02
06/22/04	06/22/04	CHEVRON #00093357 MALIBU CA D		Clothing	$15.00
Total					**-$628.21**
Total					**$392.29**

Your Rewards To Date

Travel Extras	
Prior Miles Balance	0
Miles Redeemed This Month	0
Current Miles Available for Redemption	0
Redeemable Next Month	0
Miles Earned This Month for Purchases	0
Additional Miles Earned This Month	0
Program To Date Miles Earned	2,779

Promotional Offers

Description	Current Balance	Promotional Avg Daily Balance	Promotional Rate	Promotional APR	Promotional Bal Min Pay Due	Promotional Finance Charge
PURCHASE PROMO	$0.00	$0.00	0.68460%	24.99%	$0.00	$0.00

Savings Account Summary

Finance Charges

Description	Amount
STATEMENT SAVINGS ACCOUNT BALANCE	$224.88
INTEREST PAID THIS CYCLE	$0.56

Number of Days in Billing Cycle: 29

Description	Avg Daily Balance	Daily Periodic Rate	Nominal APR	Finance Charge	Annual APR
rpt.column.Purchases	$0.00	0.08010%	29.24%	$0.00	29.24%
rpt.column.Cash Advance	$0.00	0.08215%	29.99%	$0.00	29.99%

Figure 2.20 – Statements

Figure 2.21 – Statements Category Filter

Name:	View Statement
Brief Description:	Card Member views a current or previous month's statement
Main Path:	**1.** Card Member selects view statement option on accounts summary page: **2.** Systems displays Statements page including: [B1] [B2] [B3] a. Statement Closing Date (Drop Down Box) b. Statement Summary c. Transactions d. Payments e. Purchases Finance Charges f. Cash Finance Charges g. Disclosures module h. **Actions**: Submit; Download; Disclosures; Print Friendly; Category Filter; Link (On Description) **3.** Card Member selects action: [A1] – [A9] [E1] 4. Use case ends
Alternate Paths:	**[A1]Card Member selects *Print Friendly*** 1. System displays the page of the complete statement with no HTML header or navigation 2. card member selects print from the browser **[A2]Card Member selects *Download*** 1. System invokes **Download** use case **[A3]Card Member selects *Disclosures*** 1. System displays a new pop-up page containing the Disclosures [B9] **[A4]Card Member selects a previous month's statement** 1. Card Member selects a new month 2. System displays the *Statements* page for selected month 3. System updates Activity count of statements viewed **[A5]Card Member selects Category Filter:** 1. System re-displays the *Statements* page with following data for each category: a. Category Heading b. Transactions for category c. Sub-total for category **[A6]Card Member selects link on description field of transaction:** 1. System displays pop-up including: a. Transaction Date b. Post Date c. Description d. Reference Number e. List of categories (drop down) f. Memo g. **Actions**: Close; Submit; Dispute (Link)

	2. Card Member selects category from category list and submits [A7] [A8] 3. System changes the category of the item in the database 4. System redisplays the page with the changed category **[A7]Card Member selects column heading to sort transactions:** 1. System displays page with rows sorted in default sort sequence for this column **[A8]Card Member adds a memo to a Transaction:** 1. Card Member enters text in the memo field 2. Card Member selects *Submit* 3. System saves the data and returns to *Statements* page 4. System displays transaction marked with a memo icon to show that a memo has been stored for this item **[A9]Card Member selects *dispute* link to dispute a transaction:** 1. System invokes **Dispute Transaction** use case
Exception Paths:	**[E1]** **No statement is available:** 1. System displays message stating that no statement is available
Business Rules:	**[B1]** If transactional details section contains greater than 20 lines, then paging will be invoked for this section of the statement. **[B2]** If late charge (MSR_BILL_LATE_CHG) > 0 then provide the top line of transactions with the late fee and amount. **[B3]** Display APP, Fees and Finance Charges without the transaction and post dates. **[B4]** If transaction detail type = TC 981 then display the secured card multran message detail **[B5]** If transaction code = 12 (APP, ABP, or credit insurance product) the transaction description will be truncated at byte 31 and not have a transaction/posting date or reference number. Note, this also applies to disputes. **[B6]** Merchant Category Code will be translated to 16 customized categories **[B7]** If payment has been made during the billing cycle, the system will display "No Payment Due" instead of Payment Due Date (determined by checking if STMT_MIN_PAY in CHDHDLR view is zero) **[B8]** If payment or credit is negative display amount with a negative sign in front, e.g., -$ddd.cc Display the PDF file that contains in position 3 and 4 of its title the two-byte alphabetic code that matches (non case-sensitive) the field MSR-CSF-DSCL-ID (positions 4494-4495) of the MSR file (e.g., 01aa5994.pdf corresponds to the code AA)
Notes:	Print Friendly – Shows page as it is on the statement page including the memo icon. Will show all transactions not paged Backers button will say Disclosures. It will spawn a page and display backers in PDF format. The code for determining which Disclosure to display will be characters 2 and 3 in the filename for the disclosure. Daily periodic rate: This needs to be dynamic based on code in MSR data

that determines what type of rate the card member has.

Negative amounts on transactional detail lines will be displayed with a negative sign in front of the amount (e.g., -$ddd.cc).

Category Filter will link to category view. Categories are obtained by mapping merchant SIC codes to a list of 16 categories (See mapping table for details). The category list will be:

a. Auto Related

b. Clothing

c. Computer Related

d. Dining out

e. Leisure

f. Financial

g. Groceries

h. Health Care

i. Home Repair

j. Household

k. Legal Services

l. Miscellaneous

m. Payments

n. Travel

o. Utilities

p. Work Related

For each category, the system displays a category heading followed by all the details for that category.

Transactions detail could have multiple purchases with different rates for promotion (FLAPs)

Purchases and/or cash advances may have different APR calculations based on existence of a FLAP transaction (promotion). These will be done at presentment layer, since data only contains amounts. Note that the promotional offer section differs from the Finance Charge section.

Finance charge calculations will be presented at the bottom of the Transaction Detail module. The order of presentation is: Transaction module, Savings Acct, Rewards, Promotional then Finance Charge. These are dynamic and will appear only if a card member has them.

If value of any fee is blank, then nothing should be displayed.

Statement Advertising Messages will appear at the bottom of this page.

Reference number must be restricted to range of 1 to 40 characters

2.9 Recent Activity

The recent activity use cases cover the business requirements that allow a card member to view all the transactions that have cleared since their last monthly statement was generated.

This section consists of the following use case:

- **View Recent Activity**– Allows the card member to select and view all of their recent activity.

2.9.1 View Recent Activity (320)

Figure 2.22 – Recent Activity

Name:	View Recent Activity
Brief Description:	Card Member views any transactions that have been posted since the last monthly statement was produced

Main Path:	1. Card Member selects the *Recent Activity* tab
	
	2. Systems displays *Recent Activity* page including:
	    a. Transaction Date
	    b. Post Date
	    c. Description
	    d. Category

	e. Amount 3. Use case ends.
Business Rules:	**[B1]** Card Members will not be able to add a memo to a recent transaction
Notes:	Negative amounts on transactional detail lines will be displayed with a negative sign in front of the amount, e.g., -$ddd.cc. The system will read the statement data daily batch file, repopulate Statement, delete recent activity and read new recent activity file to populate recent activity. The transactions displayed will be based on content that is available in the latest recent activity file processed by Siebel Self-Service for Cards, and will not contain transactions received by billing system after the recent activity file cut-off time. Paging will not be provided on this page

2.10 Analytics

The analytic views allow the card member to view their card history in multiple ways.

This section consists of the following use cases.

- **View Report** – Card member views standard reports or custom reports that the card member has previously defined

- **Create a Custom Report** – Card member creates and saves a report based on set of report building criteria

- **Search Transactions** – Card member creates a list of transactions based on a custom search

2.10.1 View Report (330)

Figure 2.23 – List of Reports

Figure 2.24 – Total Spending by Statement Period

Figure 2.25 – Total Spending by Statement Period Details

Figure 2.26 – Transaction History By Statement Period

Figure 2.27 – Total Spending by Category

Figure 2.28 – Total Spending by Category Details

Figure 2.29 – Top Ten Merchants

Figure 2.30 – Top Ten Merchants Details

Figure 2.31 – Top Ten Most Expensive Purchases

Figure 2.32 – Account Balance By Statement Period

Figure 2.33 – Account Balance by Statement Period Details - Card Member Statement

Figure 2.34 – Minimum Payment Due By Statement Period

Name:	List of Reports
Brief Description:	Card Member views a list of custom and standard reports.
Main Path:	1. Card Member selects the Reports tab 2. System returns *List of Reports* including: [B1] 3. List of user defined custom reports, if any. 4. List of standard reports: <blockquote>i. Total Spending By Statement Period ii. Transaction History by Statement Period iii. Total Spending By Category iv. Top 10 Merchants v. Top 10 Most Expensive Purchases vi. Account Balance By Statement Period vii. Minimum Payment Due by Statement Period</blockquote>

5. Standard Reports:

6. Card Member selects a standard report name [A1]-[A7]

7. System returns a report with a chart, in specific cases, for up to13 statement periods. [B2]

8. Card Member selects a different number of statements from the dropdown and selects Submit action to regenerate the report.

9. System returns a summary report for the selected statement period.

10. Card Member selects the Printer Friendly action.

11. System displays the page of the report without HTML header or navigational elements.

12. Custom Reports:

13. Card Member selects a custom report name.

14. System displays the details of the report using the report parameters saved for the report.

15. Card Member selects the **Edit** action.

16. System displays the saved report parameters.

17. Card Member may modify the report parameters.

18. Save under the same name or save under a new name.

19. Card Member selects the **Delete** action.

20. System displays a confirmation page.

21. Card Member selects "Yes".

22. The system removes the saved report from the list. [A8]

23. Use case ends.

Alternate Paths:	

[A1]Card Member selects Total Spending By Statement Period standard report:

1. System returns a summary report with a bar chart for up to 13 statement periods, listing the sum of the spending transactions for each statement period with a grand total amount for all periods reported.

2. Card Member selects the link to a statement period.

3. System displays the Transaction Details for the selected statement period.

4. Card Member selects the link for grand Total link for all Statement Periods.

5. System displays all Transaction Details for all statement periods listed in the report.

[A2]Card Member selects **Transaction History by Statement Period** standard report:

1. System returns the Transaction details for the previous 12 months.

[A3]Card Member selects **Total Spending By Category** standard report:

1. System returns a summary report with a pie chart for up to 13 statement periods, itemizing the amount spent on each Category with a grand total amount for all categories.

2. Card Member selects the link to a Category.

3. System displays the Transaction Details for the selected Category over the context of the statement period previously defined for the report.

4. Card Member selects grand Total link for all Categories

5. System displays the Transaction Details for all the Categories over

	the context of the statement period previously defined for the report.
	[A4]Card Member selects **Top 10 Merchants** standard report:
	1. System returns a summary report listing the Top 10 Merchants for up to 13 statement periods, listing the sum of the spending transactions for each merchant with a grand total amount for all the listed merchants.
	2. Card Member selects the link to a merchant.
	3. System displays all the Transaction Details for the selected merchant over the context of the statement period previously defined for the report.
	[A5]Card Member selects **Top 10 Most Expensive Purchases** standard report:
	1. System returns the Transactional Details listing the Top 10 Most Expensive Purchases of up to 13 statement periods in descending order by amount with a grand total for the report.
	[A6]Card Member selects **Account Balance By Statement Period** standard report:
	1. System returns a summary report with a bar chart for up to 13 statement periods, itemizing the Account Balance for each statement period.
	2. Card Member selects the link to a statement period.
	3. System displays the Statement for the selected statement period.
	[A7]Card Member selects **Minimum Payment Due by Statement Period** standard report:
	1. System returns a summary report with a bar chart for up to 13 statement periods, itemizing the Minimum Payment Due for each statement period.
	2. Card Member selects the link to a statement period.
	3. System displays the Statement for the selected statement period.
	[A8]Card Member selects "No"
	1. System returns to the save report name screen.
Business Rules:	Reports will include only statements transactions.
	All standard reports, except for Transaction History by Statement Period, are generated for the respective report based on all available statements for the card member, with the default of up to 13 months. Transaction History by Statement Period has a default of up to 12 months.
Notes:	Card Members will not have the option to download reports.

2.10.2 Create a Custom Report (340)

Figure 2.35 – Custom Report Builder

Figure 2.36 – Custom Report Results

Name:	Build a Custom Report
Brief Description:	Card Member creates and saves a custom report

Main Path:	1. Card Member selects Custom Reports tab.
	
	2. System returns a page allowing the card member to build a custom report by specifying any or all of the following report parameters:
	   a. Transaction type (Payments, Credit/Adjustment/Purchase/Cash Advance/Fees/Other)
	   b. Description
	   c. Expense Category
	   d. Transaction Amount
	   e. Time Period
	
	3. Card Member specifies report parameters and selects the **Create Report** action.
	
	4. System displays Custom Reports Results page containing the Transaction Details for the custom report requested. [B1]
	
	5. Card Member enters a report name and selects *Save* to save the custom report. [A1]
	
	6. System saves the report parameters and displays the saved report name on the *List of Reports* page under Custom Reports heading.

	7. Use case ends.
Alternate Paths:	**[A1] Card Member selects Printer Friendly** 1. System displays a page of the report without HTML header or navigational elements.
Business Rules:	**[B1]** Reports will include only statements transactions.

2.10.3 Search Transactions (345)

Figure 2.37 – Search Transactions

Figure 2.38 – Search Transactions Results

Name:	Search Transactions
Brief Description:	Card Member creates a list of transactions based on a custom search

Main Path:	1. Card Member selects *Search Transactions*
	
	2. System returns a *Search* page containing the following form fields:
	  a. Transaction Type List (All Types(default);Purchases/Debits;Credits;Payments; ATM Withdrawal)
	  b. Merchant Name
	  c. Expense Category List (All (default); See Notes in View Transactions use case for list)
	  d. Transaction Memo Contains
	  e. Transaction Amount Rule
	  f. From Date
	  g. To Date

	h. **Actions**: Search
	3. Card Member enters or selects search criteria
	4. Card Member selects a From Date and To date
	5. Card Member selects *Search*
	6. System displays Search results page
	a. Report Title
	b. Transaction Date
	c. Post Date
	d. Purchase Description
	e. Transaction Memo
	f. Purchase Amount
	g. Total
	h. **Actions**: Printer Friendly;
	7. Use case ends (card member uses tabs, sub-tabs or quick links to navigate to another page.
	a. Report Title
	b. Transaction Date
	c. Post Date
	d. Purchase Description
	e. Transaction Memo
	f. Purchase Amount
	g. Total
	h. **Actions**: Printer Friendly;
Alternate Paths:	**[A1] Card Member selects Printer Friendly**
	1. System displays the page of the report without HTML header or navigational elements.
Notes:	Search results will include transactions crossing statements and recent activity depending on the dates entered.

2.11 Secure Messages – Card Member

The secure message use cases cover the business requirements for allowing card members and CSR Users to communicate via a secured and encrypted method that serves as an alternative to e-mail or phone conversations.

This section consists of the following card member use cases.

- **Send Secure Message** – Card member sends a secure message that will be received by a Internal User

- **View Message Response**– Card member views a response from to a secure message that the card member had previously sent

- **Maintain Secure Message Inbox** – Card member maintains an "Inbox" of all secure message correspondence

2.11.1 Send Secure Message (400)

Figure 2.39 – Enter New Secure Message

Figure 2.39.1 – Enter New Message Success

Name:	Send Secure Message
Brief Description:	Card Member sends secure message to CSR User
Trigger:	Card Member does one of following: 1. Selects Send Secure Message. 2. Creates a dispute that generates a Secure Message 3. Performs an NLS query that gets no results and continues to send query as a Secure Message. (optional feature)

Main Path:	1. System displays *Send Secure Message* page containing:
	   a. Drop down list containing Message Categories
	   b. Message name
	   c. Message description
	   d. **Actions**: Submit; Clear; Cancel
	
	2. Card Member selects a Message Category from dropdown list [E1] [A1] [A3]
	
	3. Card Member enters Message Name in text box [E2]
	
	4. Card Member enters Description (full question) in text box [E3]
	
	5. Card Member selects submit to send the message
	
	6. System displays a *Secure Message Confirmation* page
	
	7. Use case ends

Alternate Path:	**[A1] Card Member selects Message Category that is covered by an online service**
	1. System displays pop-up box informing card member that service can be ordered online with link to service page
	2. Card Member selects *Continue* [A2]
	3. Use case continues from Main Path step 3.
	[A2] Card Member selects link to online service
	1. System redirects Card Member to service page
	[A3] Card Member has created a dispute:
	1. System inserts all the text from the dispute in the body of the message
	1. System submits a secure message without further card member intervention (See **Dispute a Transaction** use case)
Exception Paths:	**[E1] Card Member does not select a category:**
	1. System redisplay s page with an error messages asking Card Member to select a category.
	[E2] Card Member does not enter text for message name:
	1. System redisplay s page with an error messages asking Card Member to enter a message name
	[E3] Card Member does not enter text for message:
	1. System redisplay s page with an error messages asking card member to enter a message
Notes	The categories displayed in the pull-down menu are: Select Category; Account Balance; Account Status; Statement; Payment; APP/ABP; Other; Request Replacement Card; Add Authorized User; Change Contact Information; Order Convenience Checks; Dispute Transaction; Suggestions. These will be displayed in alphabetic order. The default should be Select Category.
	The categories that are covered by an online service are (See Section 11.12, Secure Message and Template Categories):
	1. Request Replacement Card
	2. Add Authorized User
	3. Change Contact Information
	4. Order Convenience Checks
	5. Dispute Transaction

Form Validation

NAME	DESCRIPTION	VALIDATION
*Message Name	Title of message	String Max length = 127 characters
*Description	Text of message	String Max length = 4000 characters

2.11.2 View Message Response (410)

Figure 2.40 –Message Response

Name:	**View Message Response**
Brief Description:	Card Member views a response to a previously sent secure message.
Trigger:	Card Member is notified via e-mail that their secure message has been responded to OR card member selects link from *Account Summary* page, OR card member selects message from *Message Center* page

Main Path:	1. Card Member receives an e-mail notifying them that a response has been made, containing:
	  a. Case number
	  b. Explanation

	c. **Actions**: Link to Secure Message Inbox
	2. Card Member selects link to Secure Message Inbox
	3. System prompts card member for login before redirecting card member to Message Center page
	4. System displays Secure Message Inbox sorted by date with newest message at the top:
	a. Case Number
	b. Message Name
	c. Date Entered
	d. Date Last Updated
	e. Status
	f. **Actions**: Link on Case Number Delete; New
	5. Card Member clicks case number to view message. [A1] [A2]
	6. System displays Secure Message detail page:
	a. Case Number
	b. Message Category
	c. Message Name
	d. Status
	e. Notes List (newest first)
	f. **Actions**: Reply; Delete; Close
	7. Use case ends [A3] [A2] [A4]
Alternate Paths:	**[A1] Card Member selects *New* message:**
	1. System invokes **Send Secure Message** use case
	[A2] Card Member selects *Delete* message:
	1. System deletes case
	2. System redirects card member to *Message Center* page
	[A3] Card Member selects *Reply* to message:
	1. System displays Enter New Message page with value of Case Number, Category and Message Name pre-filled and non-editable (since these values are derived from the original case)
	2. Use case continues from step 4 of **Send Secure Message** Main Path
	[A4] Card Member selects *Back*:
	1. System redirects card member to Message Center page
Notes:	Card Member has the option of reopening the case by replying to the message. A text message on the page prompts the card member to select a Reply button if the response has not answered their question.
	The Case number when the card member selects Reply to a message is the same as the case number from which it is derived. However, the case is put on the general queue and picked up by any CSR User – not necessarily the CSR User who first responded to the case. Apart from being assigned an existing case number, it is not treated differently by the system from a new message.

2.11.3 Manage Secure Message Inbox (420)

Figure 2.41 – View Message Inbox

Figure 2.42 – Message Detail

cardmanager

Contact Us | FAQs | Sign Out | Español

My Account   Payments   Self Service   Help

Ask Us a Question   **Message Center**

Quick Links

▶ Make a Payment
▶ View Statements
▶ View Recent Transactions
▶ Manage Profile
▶ Ask Us a Question
▶ Sign Out

Secure Message

Garner Mary Loug
mnambiar@edocs.com
xxxx xxxx xxxx 5838
Last Login: 02/16/2005 6:25 PM EST

View Message: #1000010

Use this page to view the response to your message and send a reply. Need more information about your original message? Click the Reply button.

To erase this message, click the Delete button. If your original problem has been solved, click the Close button.

Message Category: Dispute Transaction

Message Name: Merchandise Returned to Merchant

Message Number: 1000010

Status: Submitted

Message and Replies:

02/01/2005 11:42 PM

We will review this further.

11/30/2004 06:16 PM

Description: CHEVRON
Transaction Date: 03/08/04
Posting Date: 03/08/04
Reference Number: 2469216D62304GEPK
Amount: 25.04

Merchandise Returned to Merchant

I returned the merchandise to the merchant on 11/29/04 because Merchandise was deceptive.

Your Reply:

How much longer is this review?

Submit   Back   Clear

Figure 2.43 – Enter Message Reply
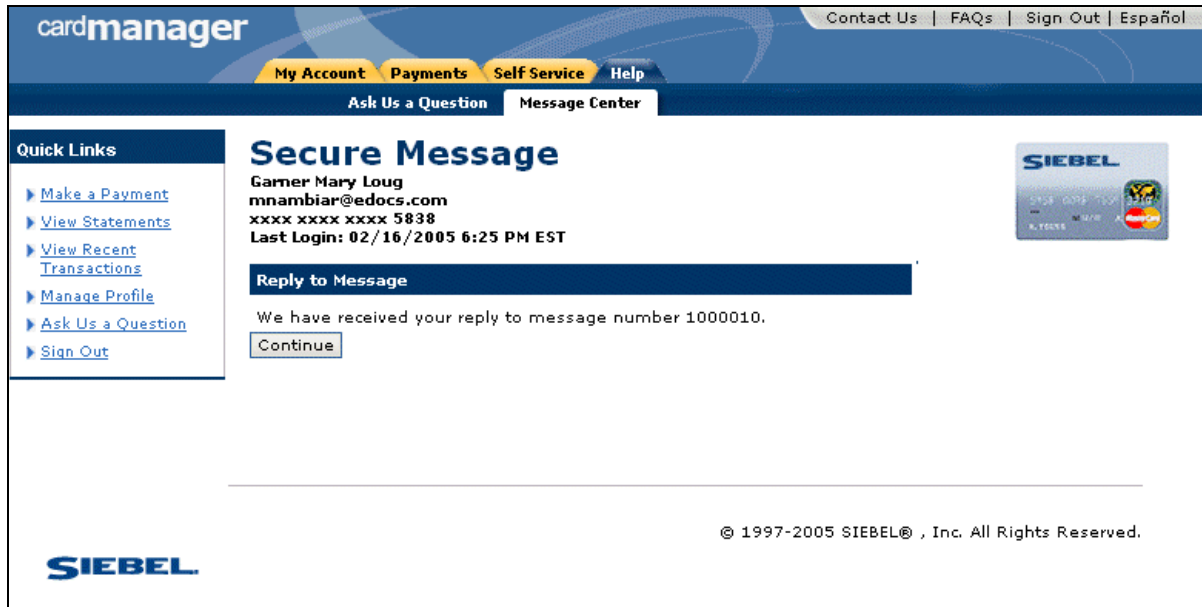
Figure 2.44 – Enter Message Reply Success

Name:	Manage Secure Message Inbox
Brief Description:	Card Member views and maintains all secure messages in an "inbox" format.

Main Path:	1. System displays a page showing secure message history
	
	2. System displays the following columns of data for each message:
	   a. Case Number
	   b. Message Name
	   c. Date and Time Entered
	   d. Date and Time Last Updated
	   e. Status (Submitted, Answered)
	   f. **Actions**: Send Secure Message; Link on Case Number; Delete
	
	3. Card Member selects a case number link [A1] [A2]
	
	4. System displays Message detail page:
	   a. Case Number
	   b. Message Category (Default: Select Category)
	   c. Message Name
	   d. Status (Submitted, Answered)
	   e. Notes List (newest first)
	   f. **Actions**: Reply; Delete; Close
	
	5. Card Member selects *Reply* action
	
	6. System displays Message Reply page:
	   a. Case Number
	   b. Message Category
	   c. Message Name
	   d. Status

	e. Notes List (newest first) f. Reply entry field (text box) g. **Actions**: Submit; Back; Clear **7.** Card Member enters values in form and submits **8.** System displays Reply Confirmation page **9.** Card Member confirms message **10.** System stores message **11.** System queues message to CSR User queue **12.** Use case ends.

Alternate Paths:	**[A1]Card Member deletes a message by selecting** *Delete***:**
	   1. System deletes message
	   2. System redisplays Message Inbox with message deleted
	
	[A2]Card Member creates a new case by selecting *New***:**
	   1. Invoke **Send New Message** use case
	
	[A3]Card Member selects *Close***:**
	System redisplays Message Inbox

Business Rule	**[B1]** Siebel Self-Service for Cards should not display messages older than 120 days.
Notes:	Secure messages can be purged after 120 days.

2.12 Manage Account

The Manage Account use cases cover the business requirements for allowing card members to manage their online profile and alerts.

This section consists of the following use cases.

- **Manage Account Profile** – Card member updates address, e-mail address and phone number information

- **Change Password** – Card member changes password

- **Manage Notifications** – Card member creates or modifies account alerts.

2.12.1 Manage Account Profile (500)

Figure 2.45 – Manage Account Profile

Figure 2.46 – Manage Account Profile Success

Name:	Manage Account Profile
Brief Description:	Card Member edits/updates their account profile including address, e-mail address and phone number.
Main Path:	1. System displays *Profile* page with the following form fields: a. Address Line 1 b. Address Line 2 c. City d. State e. ZIP Code f. Home Telephone g. Business Telephone h. E-mail Address i. Confirm E-mail Address

	j. EntPassword k. **Actions**: Submit; Cancel **2.** Card Member submits form **3.** System validates password [E1] **4.** System validates form fields: [E2] [E3] **5.** System updates account profile **6.** System sends update profile request to billing system **7.** System sends fraud alert notification [A1]-[A3] [B2] [B3] **8.** System updates activity log **9.** System redisplays page with a confirmation message.
Alternate Paths	**[A1]Address:** 1. System sends e-mail to Card Member's e-mail address 2. System sends ODS request to billing system to update mailing address 3. System logs Address change for fraud report [B1] 4. Use case continues from step 5 **[A2]E-mail:** 1. System sends card member e-mail to old and new e-mail address 2. System sends ODS request to billing system to update e-mail address 3. Use case continues from step 5 **[A3]Phone Number:** 1. System sends card member e-mail to e-mail address 2. System sends ODS request to billing system to update phone number 3. System sends ODS request to billing system to add memo to account 4. Use case continues from step 5
Exception Paths:	**[E1]** **Card Member enters invalid password:** 1. System clears form and redisplays page with an error message **[E2]** **Card Member does not enter e-mail address in a valid format:** 1. System displays message asking Card Member to enter a valid e-mail address **[E3]** **Card Member does not enter Home or Business phone number in valid format:** 1. System displays message asking card member to enter a valid Home (or Business) phone number **[E4]** **Card Member enters invalid Address:** 1. System displays message asking card member to enter a valid address
Business Rules:	**[B1]** If card member requests an address change on the same day as an enrollment, the system needs to track activity so that an entry appears in a fraud report.

	[B2]	If system event is a change of e-mail address, send a notification to both the old and new e-mail address.
	[B3]	In the event of any update to the card member's profile address, or phone number, the system will send a fraud alert notification to the card members current profile e-mail address.
Notes:	Billing system creates automatic memo for address. Billing system sends memo but next day and Fraud control needs it immediately for phone so it can contact the true owner.	
	Change Data file doesn't have address information so the only place to get it is using an ODS call. The system will store old and new address if it changes.	
	The system logs profile changes for the Activity report. There are four buckets: Address, Home Phone, Business Phone, E-mail. This is to know which fields change when the profile is changed to detect fraud. For the fraud check report, the system should determine if the streets are the same – it doesn't need to check street, city, Billing Zip.	
	Siebel Self-Service for Cards must check that State matches ZIP code. A simple algorithm that matches the first 3 digits of the ZIP code is sufficient. The same algorithm should be used in Direct Bill Pay.	

Form Validation

NAME	DESCRIPTION	VALIDATION
*E-mail Address	E-mail address of card member	Maxlength = 50, must be in xxxx@domain.xxx format.
*Home Phone	Phone number of card member with no dashes	Max length = 10 May not be all 9's or other single digit. May not have prefix 555
Business Phone	Phone number of card member with no dashes	Optional. Max length = 10
*Address Line 1	Street	Alphanumeric, space, #, dash, apostrophe, period, slash. Max length = 25
Address Line 2	Additional Address Line	Optional. Alphanumeric, space, #, dash, apostrophe, period, slash. Max length = 25
*City	City	Alphabetic, space, dash, period. Max length = 18
*State	Select from a drop-down list	Length = 2
* Zip	Zip Code	Numeric. Must be 5 digits. Must match State

2.12.2 Manage Password (510)

Figure 2.47 – Manage Password

Figure 2.48 – Manage Password Success

Name:	Manage Password
Brief Description:	Card Member changes password

Main Path:	1. System displays the *Change Your Password* Page with the following form fields:
	   a. Current Password
	   b. New Password
	   c. Re-enter New Password
	   d. **Actions**: Submit; Cancel
	2. Card Member submits form
	3. System validates password [E1]
	4. Systems stores the changed Password
	5. System displays a *Confirmation* page.
	   a. **Actions:** Next
	6. Use case ends.

Exception Paths:	**[E1] Card Member enters invalid password (see notes):** System displays error message
Notes:	Validation rules are the same as for the <u>enrollment use case</u>

Form Validation

NAME	DESCRIPTION	VALIDATION
*Password	Card Member's current password. Display is masked using asterisks.	Matches password stored by the system.
*New Password	Changed password created by card member. Display is masked using asterisks.	6-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive. New password cannot match username or secret question answers
*Confirm Password		Must be same as New Password

2.12.3 Manage Notifications (520)

Figure 2.49 – Manage Notifications

Figure 2.50 – Manage Notifications Success

Name:	Manage Notifications – Set Account Alerts
Brief Description:	Card Member configures all e-mail notifications

Main Path:	1. System displays the E-mail Alerts Page:
	    a. Checkboxes indicating current alert selections (if any)
	    b. List of available alerts:
	        i. Credit Limit Reached
	        ii. New Statement Available
	        iii. Payment is due in Reminder (1-15; default =5)
	        iv. Balance is within X amount of Credit Limit
	        v. Balance exceeds X amount
	        vi. Balance drops below X amount
	        vii. Payment posts to account
	        viii. Credit posts to account
	        ix. Transaction exceeds X amount
	        x. **Actions**: Submit; Cancel
	2. Card Member selects alerts and submits form [A1]

	3. Systems stores the list of alerts configured by the card member 4. System displays a *Confirmation* page. a. **Actions:** Next 5. Use case ends

Alternate Paths:	**[A1] Card Member deletes an alert by clearing a check box:**
	    1. System deletes the alert
	    2. System redisplays page with the alert checkbox cleared

Notes:	Card Member may configure a second e-mail address for receiving notifications other than the one on the profile. The default value for this field should be the e-mail address in the card member's personal profile. Alert notification will be driven off the Credit Limit (CL) and/or Current Balance (CB) received in the daily Billing System Change Data file as well as information in statement data and recent activity files (See Send Notification Use case for details). Credit limit (real-time) is obtained by making an ODS call to billing system at login.

2.13 Self-Service Requests

The Self-Service Request use cases cover the business requirements for allowing card members to conduct self-service function online. These card member level use cases specify the functionality required to satisfy these requirements in such a way that Siebel Self-Service for Cards can be configured, queries defined, screens developed, and any custom code developed to fulfill the use cases.

This section consists of the following use cases:

- **Order Service** – Card member requests a service.

- **Order Convenience Checks** - Card Member completes a form to have convenience checks mailed to them.

- **Request Replacement Card** – Card member requests a replacement card for an existing account

- **Add Authorized User** – Card Member adds an authorized user to an existing account.

- **Dispute a Transaction** – Card member disputes a specific transaction

- **Contact Customer Service** – Card Member views customer service contact information

2.13.1 Order Service (600)
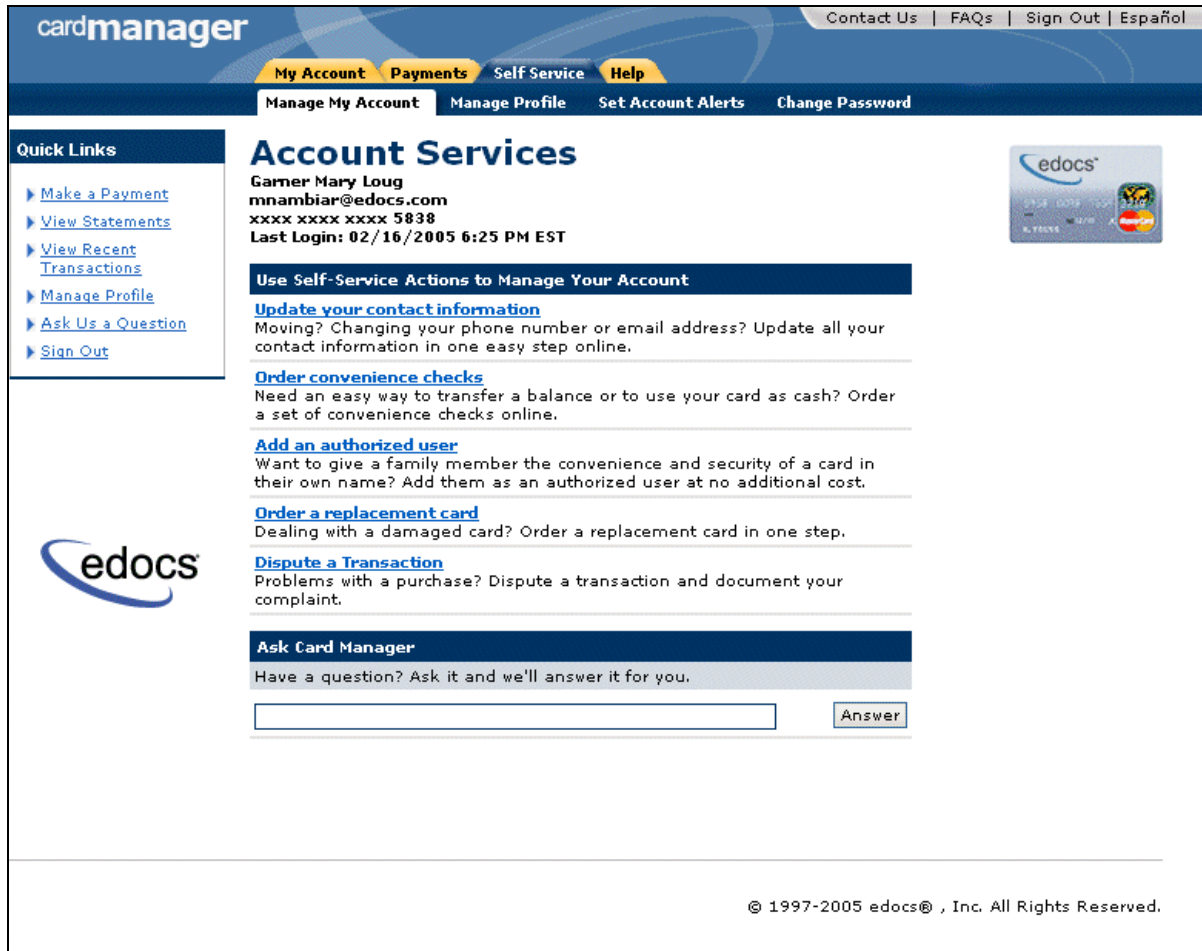
Figure 2.51 – List of Services

Name:	Order Service
Brief Description:	Card Member requests a service

Main Path:	1. System displays Self Service Requests page including: [B1]
	    a. List of services (links to service request pages)
	    b. Question (text box) (optional module)
	2. Card Member selects service [A1]-[A9]
	3. Use case ends

Alternate Paths:	**[A1] Change Contact Information:**
	    1. System invokes **Manage Account Profile** use case
	[A2] Order Convenience Checks:
	    1. System invokes **Order Convenience Checks** use case
	[A3] Request Replacement Card:

	1. System invokes **Request Replacement Card** use case **[A4] Add Authorized User** 1. System invokes **Request Additional Authorized User** use case **[A5] Dispute A Transaction** 1. System invokes **Dispute Transaction** use case **[A6] Contact Us:** 1. System invokes **Contact Customer Service** use case

Business Rules:	**[B1]** If External Status is C (closed by card member) with current balance > 0:
	
	  1. Take away all links from Services page except Dispute a Transaction and Update Your Contact Information
	
	  2. Display a generic error message at the top of the page
	
	[B2] If External Status is E (Closed) OR ((Internal Status of D (Delinquent) OR X (Delinquent and Over Limit) AND Days Delinquent > 40):
	
	  1. Take away all links from Services page except Dispute a Transaction and Update Your Contact Information
	
	[B3] If card member has a secured product type (See 11.12, Product Type Codes) card member will not be eligible to order convenience checks or Add Authorized User or Request Replacement Card and links will be removed from the list of services.
	
	[B4] If a Cardmember has MISC_THRT_ID value of "A" restrict access to services as for [B2]

Notes:	Internal Statuses are:
	  • D=Delinquent
	  • N=Credit Balance
	  • O=Over limit
	  • X=Over limit and delinquent

2.13.2 Order Convenience Checks (610)

Figure 2.52 – Order Convenience Checks Step 1

Figure 2.53 – Order Convenience Checks Step 2

Name:	Order Convenience Checks
Brief Description:	Card Member completes a form to have convenience checks mailed to them.

Main Path:	1. Card Member selects "Order Convenience Checks" from the Account Services Page
	
	2. System displays Order Convenience Checks page
	
	   a. Password (text entry box)
	
	   b. **Actions:** Submit; Cancel
	
	3. Card Member enters password and submits request
	
	4. System validates password [E1]
	
	5. System sends ODS Request using card member address on file.
	
	6. System sends e-mail notifications to card member's profile e-mail address
	
	7. System displays confirmation page
	
	8. Use case ends

Exception Paths:	**[E1] Card Member enters invalid password:** 1. System clears password field and displays error message

2.13.3 Request Replacement Card (620)

Figure 2.54 – Request Replacement Card Step 1

Figure 2.55 – Request Replacement Card Step 2

Name:	Request Replacement Card
Brief Description:	Card Member requests a replacing card for an existing account.

Main Path:	1. Systems displays a page with a form containing the following form fields: [B1] [A1]
	   a. Radio button selection for Primary OR Secondary card member
	     i. Primary Name
	     ii. Secondary Name
	   b. Password (text entry box)
	   c. **Actions**: Submit; Cancel
	2. Card Member selects Primary or Secondary, enters password and submits request
	3. System validates password [E1]
	4. System creates an ODS Request for a replacement card
	5. System displays confirmation page
	6. Use case ends.

Alternate Paths:	**[A1]Primary or Secondary Card Member's card is in the reissue process** a. System displays a message that the card is being reissued and the card member may not order another card [B2]
Exception Paths:	**[E2] Card Member enters invalid password:** 1. System clears password field and displays error message

Business Rules:	**[B1]**	Disable radio button if card is in the reissue process card member
	[B2]	The card member will not be allowed to order a replacement card if the card is in the reissue process, which is the case if the value of RESS_CNTR_CD (in the CAP view) is 4, 5, 6, 7, 8, or 9. (The card is not in the reissue process if value is 0,1,2,or 3).
Notes:	Primary and secondary names for display are obtained from CHDHLDR view (See ODS Requests). Display the name as returned by billing system.	
	There will be a text message to inform authorized users that they must call CSR User to get a replacement card, since only primary and secondary card members can use this function	
	The ODS request to order a replacement card uses the PI_EMBOSS_REQUEST_ADD RPC. (See ODS Requests for details).	

2.13.4 Add Authorized User (630)

Figure 2.56 – Add Authorized User Step 1

Figure 2.57 – Add Authorized User Step 2

Name:	Add Authorized User
Brief Description:	Card Member adds an authorized user to an existing account.

Main Path:	1. Systems displays a page with a form containing the following form fields:
	   a. First Name
	   b. Middle Initial
	   c. Last Name
	   d. Enter Password
	   e. **Actions**: Submit; Cancel
	2. Card Member enters name as it should appear on the card, enters password and submits request [B1]
	3. System validates password [E1]
	4. System validates form entry [E2]
	5. System submits ODS request for an additional card
	6. System displays confirmation page
	7. Use case ends

Exception Paths:	**[E1] Card Member enters invalid password:**
	   1. System clears password field and displays error message
	[E2] Card Member enters invalid data in name fields:
	   1. System displays error message and indicates field in error
	[E3] Card Member requests additional card for user that already

	exists: 1. System displays error message
Business Rules:	**[B1]** A card member can't request an additional card for primary and secondary card member using this function (See Request Replacement Card). Name should not match any names that are currently on that account profile.
Notes:	Primary and secondary name are in CHDHLDR view Validate that requested name is not already an authorized user by selecting CUST_NM from CAP view (See ODS Requests for details). Use the CUSTOMER_ADD RPC to add the additional authorized user (See ODS Requests for details).

Form Validation

NAME	DESCRIPTION	VALIDATION
* Name	First Name of card member as it will appear on the Card	Alphabetic, spaces or hyphens. Max. length = 10 Min length = 1
Middle Initial	Middle Initial as it will appear on the card	Alphabetic Length = 1
*Last Name	Last Name of card member as it will appear on the Card	Alphabetic, spaces or hyphens Max length = 15 Min length = 1

2.13.5 Dispute A Transaction (650)

cardmanager

| My Account | Payments | Self Service | Help |

Manage My Account   Manage Profile   Set Account Alerts   Change Password

Quick Links

▶ Make a Payment
▶ View Statements
▶ View Recent Transactions
▶ Manage Profile
▶ Ask Us a Question
▶ Sign Out

SIEBEL

Disputes

Garner Mary Loug
mnambiar@edocs.com
xxxx xxxx xxxx 5838
Last Login: 02/16/2005 6:25 PM EST

Dispute Transaction   Step 1 of 2

To complete your dispute, review the transaction information below and complete the dispute documentation.

Description: BU SHOE DEPT 395   WALDORF   MD

Transaction Date: 06/19/04   mm/dd/yy

Posting Date: 06/19/04   mm/dd/yy

Reference Number: 7473068E20258X7T7
(17-digit code from statement)

Amount: $ 50.00   (in dollars and cents)

Please select the reason for your dispute below:

○ Non Receipt of Ordered Merchandise
○ Shipped Merchandise is Defective or Not as Described (by the merchant)
○ Merchandise Returned to Merchant
○ Duplicate Billing (billed twice or more by the same merchant)
○ Incorrect Transaction Amount
○ Hotel/Motel Reservation Cancelled Prior to Stay
○ Cancellation of a Recurring Transaction
◉ Unauthorized Transaction(s)
○ Credit was not Received from Merchant

If the reason for your dispute is not listed above,
please contact Cardmember Service at 1-800-555-1212.

[Next] [Cancel]

Billing Rights Summary

Tips

Easy Way to Make Disputes
Use CardManager to help you fill out your dispute.

- Go to your statement.
- Scroll to the Transactions section. Click on the merchant/ transaction description of the transaction you wish to dispute.
- In the pop-up window, click the Disputes link. This link will bring you back to this page with the transaction information automatically filled in for you.

SIEBEL

© 1997-2005 SIEBEL® , Inc. All Rights Reserved.

Figure 2.58 – Dispute Transaction – Step 1

Figure 2.59 – Dispute Transaction – Step 2

Figure 2.60 – Dispute Transaction Confirmation – Step 3

Name:	Dispute A Transaction
Brief Description:	Card Member disputes a specific transaction

Main Path:	1. System displays *Disputes* page containing the following form fields:
	   a. Description
	   b. Transaction Date
	   c. Posting Date
	   d. Reference Number
	   e. Amount
	   f. Reason Selection list
	   g. **Actions**: Next; Cancel
	2. Card Member completes form and selects *Next*
	3. System displays *Disputes* Page 2: [E1]
	   a. Summary information
	   b. Home Phone
	   c. Business Phone
	   d. **Actions**: Submit; Edit; Cancel

	4. Card Member enters text for specific dispute
	
	5. System displays *Disputes* Page 3 (confirmation):
	    a. Information from previous page (full text of dispute)
	    b. **Actions**: Printable Version
	
	6. System generates a secure message with category of *Dispute* (See **Send Secure Message** use case)
	
	7. Use case ends [A1].

Alternate Paths:	**[A1]Card Member selects link to print the page**
	    1. System displays a page without navigation
	    2. Card Member uses browser print function to print the page

Exception Paths:	**[E1] Card Member enters invalid field:** 1. System displays error message

Notes:	All the dispute information is on the confirmation page: the radio button text becomes a sentence and is combined into a text field. Options are:
	    1. Not Received Merchandise
	    2. Merchandise Defective
	    3. Sent Defective Date Selection
	    4. Charged Twice
	    5. Billed Wrong Amount
	    6. Cancelled Reservation
	    7. Cancelled Subscription
	    8. Credit for Transaction Not Shown
	
	Home and work phone numbers will be pre-filled using values from the card member's personal profile
	
	Reference number must be restricted to range of 1 to 40 characters

2.13.6 Contact Customer Service (680)

Figure 2.61 – Contact Us Page

Name:	Contact Customer Service
Brief Description:	Card Member views customer service contact information
Main Path:	1. Card Member selects *Contact Us* 2. System displays a page containing information for contacting customer services depending on card member's product type code. 3. Use case ends
Notes:	This page contains static content only. But different phone numbers will be displayed depending on the values of the product type code as well as the card member's language. (See Section 11.12, Product Type Codes) No session information is required.

2.14 Static Content

The static content use cases cover the business requirements for allowing card members to view help information and static content online. This section consists of the following use cases:

- **View Credit Tips** – Card member views credit tips from the Resource Center .

2.14.1 View Credit Tips (690)

Figure 2.62 – Credit Tips

Name:	View Credit Tips
Brief Description:	Card Member views and links to Credit Tips page.
Main Path:	1. Card Member selects Credit Tips tab. 2. System displays a page containing a link to Credit Tips. 3. System links to a popup window card member which serves the Credit Tips 4. Use case ends.
Notes:	This page contains links and static content only. No session information is required.

2.15 Payment Use Cases

The payment use cases cover the business requirements for allowing card members to pay charges from their statements.

This section consists of the following use cases.

- **Make A Payment** – Card Member completes an online payment.

- **Manage Bank Account** - Card Member selects *Payment Account* sub-tab OR card member selects *Make Payment* function and does not have an existing Payment Account

- **View Payment History** – Card Member views a list of payments made, views the receipts for online payments and manages scheduled payments

- **Manage Payees -** Card Member adds, edits or deletes payee information for use in Pay Other Bills payment

- **Make Pay Other Bills Payment** – Card Member makes a Pay Other Bill payment

2.15.1 Make A Payment (700)

Figure 2.63 – Make A Payment – Step 1

Figure 2.64 – Review Payment – Step 2

Figure 2.65 – Payment Confirmation – Step 3 Manage Bank Account (730)
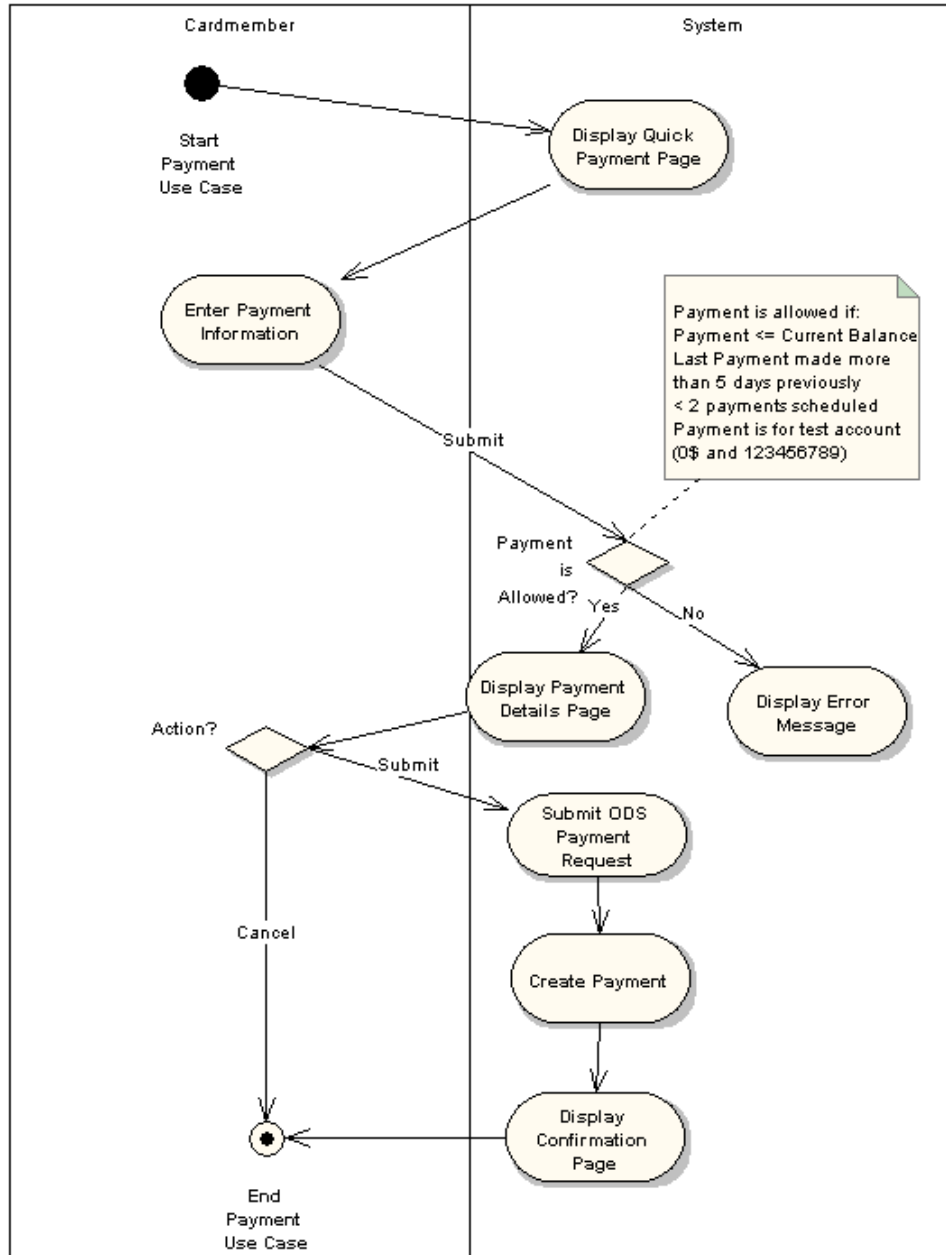
Figure 2.66 –Payment Activity

Name:	Make A Payment
Brief Description:	Card Member completes an online payment
Main Path:	1. System displays *Make A Payment* Screen containing the following fields: [B4] a. Total Credit Limit b. Account balance

   c.   Available Credit

   d.   Payment Due Date

   e.   Past Due Amount

   f.   Amount Over Credit Limit

   g.   From Payment Account

      i. Bank Account

      ii. Bank Account Number (masked except for last 4 digits)

   h.   Radio buittion selection of:

      i. Minimum Payment;

      ii.Statement Balance;

      iii.   Specified amount

   i.   Payment Notification (Default: checked)

   j.   **Actions**: Next; Cancel; <u>Add/Change Bank Account</u>

2. Card Member selects:

   a.   Statement Account Balance OR Minimum Amount Due (Default) OR Card Member entered amount

   b.   Payment Notification

3. Card Member selects *Next*

4. System displays a Review Payment Information page with: [A1] [A2] [A3][B1] [B2] [B3] [B5] [B6][E1]

5. Bank Account

6. Payment Amount Type (Account Balance; Minimum Payment; Specified Amount)

7. Payment Amount

8. Payment Notification Flag

9. **Actions**: Submit; Edit; Cancel

10. Card Member submits payment [A5]

11. System submits <u>[ODS payment request](#)</u> [E2]

12. System creates payment [E3]

   a.   Bank Account

   b.   Amount paid

   c.   Date of payment

   d.   Payment Notification Flag

   e.   Confirmation Number

13. System displays a *Payment Confirmation* page showing:

14. Use case ends

Alternate Paths:	**[A1]Card Member selects *Edit* to modify payment:**
	1. System displays Make A Payment Step 1 with previous values retained

Exception Paths:	**[E1] Card Member enters invalid data in form fields:**
	1. System displays the input form containing previously entered fields and a message indicating that input was invalid
	[E2] System fails to complete ODS payment request:
	1. System redisplays the input form with error message indicating

	failure
	[E3] System cannot process the payment:
	1. System redisplays the input form with error message indicating failure.
	[E4] Card Member has not set up a bank account:
	1. System displays an error messaging requesting that the card member enter bank account information before making a payment.
Business Rules:	**[B1]** Card Member will not be allowed to make a payment greater than the current account balance.
	[B2] If Min Payment Due is zero, the page will display a message "No payment due" instead of payment due amount.
Notes:	System captures account information at login for the account summary section (See Account Summary Data table for these calls)
	Payment processing is assumed to occur only on business days.
	Payment page will include specialized help function to walk card member through the payment process.
	There will be a business day and holiday disclaimer on all steps one and three of all three payment functions.
	EPICWare is used only at enrollment or when modifying bank account information to ensure that this information is correct.
	Display masked bank account number directly under Bank Account Nickname but with no title.
	If card member does not have an existing bank account and selects Make a Payment function, display a message at the top of the page (similar to an error message) saying something like, "You have not yet provided bank account information. Please click the Add/Change Bank Account Link to set up a Bank Account."
	Payment Date is misleading on One-Time Payment page because only today's date is allowed, so this field will be suppressed for one-time payments.

Form Validation

NAME	DESCRIPTION	VALIDATION
Payment Amount	Amount to be debited from the card member Account	Defaults to the minimum amount due from the most current bill Greater than $1.00 Amount must include cents. Strip out any commas.
Payment Date	Date the payment will be processed	At least today Less than or equal to 60 days in future. Only today (Phase 1)

2.15.2 Manage Bank Account (730)

Figure 2.67 – Payment Account

Figure 2.68 – Add Bank Account Step 1

Figure 2.69 – Add Bank Account Step 2

Figure 2.70 – Edit Bank Account Step 1

Figure 2.71 – Edit Bank Account Step 2

Figure 2.72 – Delete Bank Account

Name:	**Manage Bank Account**
Trigger:	Card Member selects *Payment Account* sub-tab OR card member selects *Make Payment* function and does not have an existing Payment Account
Brief Description:	Card Member adds, edits or deletes bank account information for use in making payments.

Main Path:	1. Card Member has not yet configured a payment account and selects *Add Account* [A1]
	
	2. System displays *Add Payment Account* page:
	  a. Bank Name
	  b. Bank Account Nickname
	  c. Routing number
	  d. Confirm routing number
	  e. Account number
	  f. Confirm account number
	  g. Account type (Checking OR Savings)
	  h. **Actions**: Next; Cancel
	
	3. Card Member enters and selects Next
	
	4. System displays *Review Payment Account Information:*
	  a. Bank Name
	  b. Bank Account Nickname
	  c. Account type
	  d. Routing number
	  e. Account number
	  f. **Actions**: Submit; Edit; Cancel
	
	5. Card Member submits bank information
	
	6. System invokes **Validate Banking Information** use case [E1] [E2]
	
	7. System sends ODS request to update banking information at the billing system
	
	8. System sends e-mail notification to card member's profile e-mail address
	
	9. System stores bank information for use in future payments
	
	10. System redirects card member to the *Payment Account* page and displays the payment account information for the added account
	
	11. Use case ends.

Alternate Paths:	**[A1]Card Member already has a bank account:**
	  1. System displays the *Payment Account* page with current payment information:
	    a. Bank Account Nickname
	    b. Account Type (Checking or Savings)
	    c. Account number (masked except for last 4 digits)
	    d. Expiration date
	    e. **Actions**: Edit; Delete;
	  2. Card Member selects Edit [A2]

3. System displays *Edit Payment Account* page:

   a. Bank Name

   b. Bank Account Nickname

   c. Account Type (Checking, Savings)

   d. Routing number

   e. Confirm routing number

   f. Bank account number

   g. Confirm account number

   h. **Actions**: Submit; Edit; Cancel

4. Card Member modifies bank account information and selects Submit

5. System displays Edit Payment Account confirmation page:

   a. Bank Account Nickname

   b. Account type (Checking, Savings)

   c. Routing number

   d. Bank account number

   e. **Actions**: Submit; Edit; Cancel

6. System invokes **Validate Banking Information** use case [E1] [E2]

7. System sends ODS request to update banking information at the billing system

8. System stores modified bank account information

9. System sends an email notification to card member's profile address that bank account number or routing number has been changed

10. System redirects card member to the *Payment Account* page and displays the payment account information for the edited account

[A2]Card Member selects *Delete* to remove bank account:

1. System displays a confirmation page: [A3]

   a. Message stating that this action will delete all scheduled and recurring payments

   b. Payment account name

   c. Account number (masked except for last 4 digits)

   d. Actions: Delete; Cancel;

2. Card Member selects Delete

3. System sends ODS request to billing system to delete bank account

4. System deletes all pending payments and recurring payments

5. System deletes the account and redisplays the *Payment Account* page with no payment account and Add Account button

Exception Paths:

[E1]   Card Member enters invalid bank information:

1. System displays page with previously entered information and a message requesting card member to enter a valid routing number

2. Use case ends

[E2]   EPICWare repairs Bank information

1. System displays a message telling the card member that the bank account information was repaired and corrected information

2. Card member confirms that bank information is correct

	3. Use case continues from Main Path Step 6
Business Rules:	**[B1]** Account number will be masked except for last 4 digits on all displays except when entering the first time. **[B2]** Only one bank account per card member account (so that system can't overwrite payments in billing system) **[B3]** If Bank account already exists, the Add Bank Account button will be suppressed. **[B4]** If card member does not have any Bank Account configured and selects the Manage Bank Account function, redirect CM to the Add Bank Account page.
Notes:	The application will make a call to FT EPICWare to validate the DDA and ABA routing number but only when card member adds or modifies bank account information. EPICWare returns a simple table of codes. Once passed on EPICWare the system will send account type, DDA, ABA to billing system. Graphics for Routing Number and Account Number will be displayed on the page. Bank account numbers are stored locally and are sent to billing system only when modified. The system deletes bank account at billing system by sending the same update request with blank fields. Since the card member can currently only enter one bank account and the card member is redirected to the Add Bank Account page if no bank account has been set up, the Add Account module will never be displayed in the phase 1 implementation. Bank Name field was added because it is needed for ACH payments. Bank Name is required, but Bank Nickname is optional.

Form Validation

NAME	DESCRIPTION	VALIDATION
*Bank Account Nickname	Friendly Name or Nickname	32 Characters
*Routing Number	Bank routing number	9-Digit Routing number checked according to ACH rules (hash and check digits) Call made to EPICWare subsystem to validate against ABA number.
*Routing Number (Repeated)	Bank routing number	Must be same as previous field
*Bank Account Number	Bank account number	Maximum length 17 Digits (but can be less) Call made to EPICWare subsystem to validate DDA number

*Bank Account Number (Repeated)	Bank account number	Must be the same as previous field
Account Type	Type of account	Checking (default) or Savings

* Indicates required field

2.15.3 View Payment History (740)

Figure 2.73 – Payment History

Name:	**View and Manage Payment History**
Brief Description:	Card Member views a list of payments made, views the receipts for online payments and manages scheduled payments

Main Path:	1. System displays *Payment History* Page:
	   a. Date
	   b. Bank Account (Nickname)
	   c. Payment Type
	   d. Payment Function (Minimum, Current, Specific)
	   e. Status (scheduled, processing, submitted)

	f. Confirmation number g. Amount h. **Actions**: Cancel **2.** Use Case ends
Notes:	Payment history will display Payment function (minimum, statement balance, or specified amount) in addition to usual payment information. This will be stored in flexible fields with other payment information.

2.15.4 Manage Payees (750)

Name:	**Manage Payees**
Brief Description:	Card Member adds, edits or deletes payee information for use in Pay Other Bills payment

Main Path:	1. System displays the *Payees* Screen displaying a list of current payees that have been set up with account information and form for making up to four payments: [B2] [B4]
	    a. Payee account name (Up to 4 drop downs)
	    b. Amount (Up to 4 entry fields)
	    c. **Actions** Next; Clear; Learn more
	    d. Payee name
	    e. Payee account number (masked except for last 4 digits)
	    f. **Actions**: Edit; Delete; Add Payee
	2. Card Member selects *Add Payee* [A1], [A2] [A3]
	3. System displays the *Add Payee* Screen displaying:
	    a. Name
	    b. Address
	    c. City
	    d. State
	    e. Zip Code
	    f. Payee Account Number
	    g. **Actions**:Next; Cancel
	4. Card Member enters Payee information and selects *Next*
	• System validates Payee information[E1] [E2] [B5]
	• System displays *Review* page:
	    a. Account summary information
	    b. Payee information
	        a. **Actions**: Submit; Edit; Cancel
	• Card Member confirms addition of new payee [A4]
	• System stores payee information for use in future payments
	• System redisplays *Payee* page with added Payee information
	• Use case ends.

Alternate Paths:	**[A1]Card Member selects** *Edit* **to modify list of payees:**
	   1. System displays the *Edit Payee* Page:
	      a. Name
	      b. Address
	      c. City
	      d. State
	      e. Zip Code
	      f. Account Number (Masked)
	      g. **Actions**: Clear; Next
	   2. Card Member makes edits and selects *Next*
	   3. System checks that account number is not the card member's account account [E1] [E2] [B5]
	   4. System displays *Confirmation* page:
	      a. Account summary information
	      b. Payee information
	      c. **Actions**: Cancel; Back; Submit
	   5. Card Member confirms edits
	   6. System stores updated payee information
	   7. System redisplays *Payee* page with modified Payee information
	
	[A2]Card Member selects *Delete* **to delete payee from list**
	   1. System displays *Review* page:
	      a. Payee information
	      b. **Actions**:Submit; Cancel
	   2. Card Member confirms deletion
	   3. System deletes payee record
	   4. System displays *Current Payment Accounts* list with payee removed
	
	[A3]Card Member selects Make Payment to make a Pay Other Bills payment:
	   1. System invokes **Pay Other Bills Payment** use case
	
	[A4]Card Member selects Cancel on *Review* **payees page:**
	   1. System displays *Payees* page

Exception Paths:	**[E1] Card Member enters invalid Zip and State:**
	   1. System displays message "The Zip Code you entered is not valid for the state you entered. Please try again."
	
	[E2] Card Member enters invalid Account Number:
	   1. System displays a message that the account number is invalid

Business Rules:	**[B1]** Account number should be masked **[B2]** If ODS is down Pay Other Bills pages will be modified according to notify that this feature is unavailable and to try again later. **[B3]** Check External status codes follow certain rules (See business rule for Make Pay Other BIlls Payment).
Notes:	System will pull all information for business rules from CHDHLDR and

	CARDHOLDER_NAME view at login

Form Validation

NAME	DESCRIPTION	VALIDATION
*Payee Name	Name of payee	Alphanumeric. Max Length = 26
*Address	Address Line 1	Alphanumeric. Max Length = 26
*City	City	Alphanumeric. Max Length = 18
*Zip Code	Payee Zip Code 5 + 4	Numeric Length = 9 Minimum Length = 5
*Payee Account Number	Payee Account Number	Character. Max Length = 21

* Indicates required field

Figure 2.74 – Pay Other Bill Payees

Figure 2.75 – Add Payee Step 1

Figure 2.76 – Add Payee Step 2

Figure 2.77 – Add Payee Success

Figure 2.78 – Edit Payee Step 1

Figure 2.79 – Edit Payee Step 2

Figure 2.80 – Edit Payee Success

Figure 2.81 – Delete Payee Step 1

Figure 2.82 – Delete Payee Step 2

2.15.5 Make Direct Bill Payment (760)

Figure 2.83 Pay Other Bills Payment – Step 1

Figure 2.84 – Pay Other Bills Payment – Step 2

Figure 2.85 – Pay Other Bills Payment – Step 3

Name:	Make Pay Other Bills Payment
Brief Description:	Card Member makes a Pay Other Bill payment
Trigger:	Card Member navigates to Make Direct Bill Payment page

Main Path:	1. System displays the *Pay Other Bills* page displaying a list of current payees that have been set up with account information and form for making up to four payments:
	
	   a. Payee account (Up to 4 drop downs)
	   b. Amount (Up to 4 entry fields)
	   c. **Actions**: ; Next; Clear
	   d. Payee Name
	   e. Account number (masked except for last 4 digits)
	   f. **Actions**: Edit; Delete; Add Payee
	
	2. Card Member selects up to 4 payees and enters a payment amount for

	each
	3. Card Member selects *Next*
	4. System validates form input and checks that credit is available [E1]
	5. System redirects card member to *Review* Payment page:
	a. Payee Name
	b. Payee Address (Street, City, State, ZIP)
	c. Account Number
	d. Amount
	e. Agree To Terms
	f. **Actions**: Submit; Back; Cancel, Agree To Terms
	6. Card Member checks Agree To Terms and submits payment [E2]
	7. System sends an ODS request (Balance Transfer) request to make each payment [E3]
	8. System sends e-mail to profile e-mail address
	9. System displays *Confirmation* page displaying same information as *Review Payment* page with a note next to each payment stating Payment Submitted or Payment Failed
Exception Paths:	**[E1] Card Member enters one or more invalid input fields:**
	1. System displays the input form containing previously entered fields and a message indicating that input was invalid
	[E2] Card Member does not check Agree To Terms
	1. System redisplays page with a message stating that the card member must agree to terms
	[E3] System ODS request fails:
	1. System displays error message
Business Rules:	**[B1]** The number of available Payees for Make Payment (i.e., the number of drop-down selection boxes will be the same as the number of Payees that have been added up to a maximum of four.
	[B2] Terms are decided on basis of Misc 10 field: Z =90days (only one working currently)
	[B3] Show Pay Other Bills tab if eligible:
	1. Misc Field 10 Position 1 is Z
	2. External Status of " " (blank)
	3. Internal Status of " " (blank) or "N"
	4. NOT Statement Hold Code of "R"
	5. NOT Auth Flag of "A"
	6. NOT # of Plastics of "0"
Notes:	System will obtain Flags from the billing system at login:
	• CHDHLDR Misc Field 10 Position 1:
	• CHDHLDR External Statuses: blank
	• CHDHLDR Internal Statuses: blank, N
	• CHDHLDR Statement Hold Code: Not R
	• CHDHLDR Auth Flag: Not A
	• CAP Plastics Count: Not 0

	Each payment is a separate ODS Call
	In order to process a 90 days seamless cash the billing system also needs a ticket terms code. Ticket terms code is 5232.
	If any of the ODS calls fail the *Payment Submitted* is currently highlighted in red. The card member has to try again.
	Siebel Self-Service for Cards must collect information confirming card member's agreement to terms and conditions and save this permanently to answer potential future queries (like an electronic signature). The information saved will allow a query that returns for all card members that have accepted terms and conditions: User ID, SSN, Timestamp, Type of agreement (Paper off, Direct bill payment)

Form Validation

NAME	DESCRIPTION	VALIDATION
Payment Amount	Amount to be paid.	Must be > or = $5.00 and < or = $4,000

2.16 System Use Cases

The system use cases cover the business requirements for actions initiated by the system based on configurations or jobs set up by the system administrator.

This section consists of the following use cases.

- **Read and Store Card Member Account and Status Information** – System collects account information from the billing system and stores it for later use to drive navigation.

- **Validate CVC/CVV Number** – System validates CVV/CVC number entered by card member against CVV/CVC number stored by the billing system.

- **Upload User Profile -** System uploads User Profile to transition card members from the existing Incurrent database into the Siebel Self-Service for Cards database.

- **Upload Pay Other Bills Payee Data –** System uploads Bill Payee data for Pay Other Bills function to transition card members from the existing Incurrent database into the Siebel Self-Service for Cards database.

- **Decrypt Password** – System decrypts password on migrated user profile file.

- **Upload CHD Data** – System reads the <u>daily Change Data (CHD) file</u> sent from the billing system to update Siebel Self-Service for Cards with changes that have been made to online accounts through FDR processes. System generates alerts based on card member preferences and system configuration.

- **Upload MSR Data** – System reads the daily statement cycle (MSR) file sent from FDR to update Siebel Self-Service for Cards with statement data.

- **Upload MON Data** – System reads the daily Monetary (MON) file sent from FDR to update Siebel Self-Service for Cards with recent account activity.

- **Send E-mail Notification** – System sends an e-mail to notify the card member of a system event (See Appendix A – E-Mail Notifications), for example, that the statement is available, or a card member configured alert has been triggered.

- **Log User Activity** – System logs card member and CSR User activity

- **Create Management Report** – System creates a management report on request (either by Scheduler or Administrator).

- **Validate Banking Information** - System calls EPICWare software to validate a pair of DDA and ABA numbers. EPICWare software returns a success or error code and, in some cases, a repaired ABA number.

2.15.1 Read and Store Card Member Account and Status Information (900)

Name:	Read and Store Card Member Account and Status Information
Brief Description:	System collects account information from the billing system and stores it for later use to drive navigation
Main Path:	1. System calls ODS to retrieve card member information using Account Number and stores it for use in card member session: [E1] [E2] a. Primary Name b. Secondary Name c. External and Internal Status Codes d. Paper Off Eligible Flag e. Paper Hold Flag f. Card Code (for brand) g. Direct Bill Pay Eligible Flag h. Balance Transfer Eligible Flag i. Billing Zip Code j. Address k. Product Type Code (for secured card) l. Payment Due Date m. Minimum Payment Due n. Past Due Amount o. Amount Over Credit Limit p. Last Payment Amount q. Last Payment Credited Date r. Current Available Credit s. Current Available Cash Advance t. Recent Activity (Pending Transactions) u. Credit Limit v. Current Balance 2. System stores Social Security Number in Siebel Self-Service for Cards database for use in locating card member account by SSN for the *card member Profile* page [A1] [A2] 5. Use case ends

Alternate Paths:	**[A1] Card Member is already enrolled and logs in:**
	1. System calls ODS to get e-mail address and stores it for use in card member session
	2. Use case ends
	[A2] Card Member enrolls:
	1. System calls ODS to get:
	a. Social Security Number
	b. Expiration Dates
	c. Card Member Name (as on the card) for name validation
	2. Use case continues from Main Path step 2
Exception Paths:	**[E1] Account number doesn't exist at the billing system:**
	1. System sets error message and return code
	[E2] System ODS request fails:
	1. System will return an error message asking card member to try again later
Notes:	If Siebel Self-Service for Cards does not already have card member's SSN (card member is enrolling or is being migrated from Incurrent system, then Siebel Self-Service for Cards must store the SSN in its database so that CSR Users can perform a query for card member accounts by SSN.

2.15.2 Validate CVC/CVV Number (901)

Name:	**Validate CVC/CVV Number**
Brief Description:	System validates CVV/CVC number entered by card member against CVV/CVC number stored by the billing system
Main Path:	1. System reads the CVV/CVC numbers of cards issued to the card member and checks them against the CVV number entered by the card member. (See business rules, [B1] [B2])
	2. Use case ends
Business Rules:	**[B1]** Validate CVV: Check expiration reissued expiration and manually updated expiration in turn and if all three fail the validation fails. (See also example code.) Use following logic:
	1. Call ODS to get name, soc sec, expiration date, Billing Zip Code from CHDHDLR view
	2. Call ODS to get available CVV/CVC values from EMBOSS_TEMP view using expiration date information from step a.
	3. Check CVV matches CVV provided by user.
	[B2] CVV code of "000" is a valid code. If expiration date is "00000000" don't use it (e.g., for new cards not all expiration dates are set)

2.15.3 Upload User Profile (910)

Name:	Upload User Profile
Brief Description:	System uploads User Profile to transition card members from the existing Incurrent database into the Siebel Self-Service for Cards database

Main Path:	1. System reads User Profile data:
	    a. Card Member Account Number
	    b. Login ID
	    c. Password
	    d. E-mail Address
	    e. Bank Account Number
	    f. Routing Number
	    g. Language Preference
	    h. Locked Flag
	    i. Disabled Flag
	2. Decrypt Password
	3. System converts Password to upper case
	4. System stores User Profile data in Siebel Self-Service for Cards database
	5. Use case ends

Notes:	Field separator will be "||" (double pipe) Account Protection Plus Not Needed in User Profile file but pre-fill Confirm fields during detailed design

Card Member Profile Format

NAME	DESCRIPTION	LENGTH
Card Member Account Number	Numeric	16
Card Member Login ID	String	30
Password	String	12
E-mail Address	String	50
Bank Account	Numeric	17
Routing Number	Numeric	9
Language Preference	Boolean	1
Locked Flag	Boolean	1
Disabled Flag	Boolean	1

2.15.4 Upload Pay Other Bills Payee Data (920)

Name:	**Upload Direct Bill Payee data**
Brief Description:	System uploads Bill Payee data for Pay Other BIlls function to transition card members from the existing Incurrent database into the Siebel Self-Service for Cards database

Main Path:	1. Upload Payee data:
	    a. Account Number
	    b. Payee Account Number
	    c. Payee Name
	    d. Address Line 1
	    e. City
	    f. State
	    g. Zip Code
	2. System stores Payee data
	3. Use case ends

Notes:	Multiple payees per card member. 2000 enrolled users with around 700 actively used. Field separator will be "||" (double pipe)

Payee Data Format

NAME	DESCRIPTION	LENGTH
Card Member Account Number	Numeric	16
Payee Account Number	String	21
Payee Name	String	26
Address Line 1	String	26
City	String	18
State	String	2
Zip	Numeric	9

2.15.5 Decrypt Password (921)

Name:	**Decrypt Password**
Brief Description:	System decrypts password on migrated user profile file.
Main Path:	1. System reads password

	2. System decrypts password **3.** Use case ends
Notes:	The decryption key and algorithm for decrypting password is configurable for each engagement,

2.15.6 Upload CHD Data (970)

Name:	**Upload CHD Data**
Brief Description:	System reads the daily Change Data (CHD) file sent from the billing system to update Siebel Self-Service for Cards with changes that have been made to online accounts through FDR processes. System generates alerts based on card member preferences and system configuration.
Main Path:	**1.** System reads transactions from CHD file: a. For each record, system determines whether an e-mail notification is required and sends e-mail according to rules defined in Send E-mail Notification use case: i. Credit Limit Reached ii. Balance is Within $X of Credit Limit iii. Balance Exceeds $X iv. Payment due in X days v. Balance drops below $X b. For each change to bank information, System updates the card member's bank account information, sends an e-mail to the card member's account profile e-mail address c. For each change of account due to lost or stolen credit card, make update to card member's Account Number. (See Account Transfer Logic for the logic associated with this business process.) d. For each e-mail address change, update Siebel Self-Service for Cards database with changed e-mail address. e. For each new card member account create an entry in the Siebel Self-Service for Cards database so that card member can enroll.
Notes:	If bank account changes, a record will be created in the Change Data (CHD) file containing account type DDA, ABA. Billing system may deliver files in any sequence. Billing system will deliver a file even if it contains no records. Billing system e-mail address format in the Change Data file is: • HOME-EMAL-ADDR-TX X(50) • HOME-EMAL-SLCT-IN X • HOME-EMAL-STTS-IN X • HOME-EMAL-OPRT-ID X(4) • HOME-EMAL-TRMN-ID X(4) However, HOME_EMAL_ADDR_TX is the only field Siebel Self-Service for Cards needs to store. E-mail indicators will always be set to the same values on outgoing messages. Operator and Terminal ID will not be used.

CHD File Format

The CHD data file is a modified version (subset) of the CHD file as defined by the FDR document, "COMBINED CARDHOLDER MASTER AND FLAP FILE (095)" Version "03.9.4 – MAJOR." See below for a list of the fields used by Siebel Self-Service for Cards. For full file specification, see Appendix G – CHD File Format

ID	NAME	DESCRIPTION
1	Account Number	Primary Key for card member account. If this Account Number is not already enrolled, Siebel Self-Service for Cards will assume that this is a new account and create a new entry in the database.
4	Transit Routing Number	Use to update card member's Bank Account information in the Siebel Self-Service for Cards database
5	Checking Account Number	Use to update card member's Bank Account information in the Siebel Self-Service for Cards database
6	Savings Account Number	Use to update card member's Bank Account information in the Siebel Self-Service for Cards database
7	Credit Line	Used for alerts
9	Cross Ref Account Number	Account Number Reference. For Lost & Stolen. (Contains new account number before Account Transfer Date, blank after that date)
11	New XREF Number 2	Additional Account Name Reference. For Lost & Stolen. (Contains old account number on Account Transfer Date, blank before this date)
12	Account Transfer Date	For Lost and Stolen. This is the date the actual transfer to the new account will take place. On this date the transfer will be completed, Siebel Self-Service for Cards should use the new account number (which will be in the Account Number field) for all transactions and the field will be blank.
14	Payment Due Date	For payment due notification
18	Current Balance	For alert
21	E-mail Address	Present if an CSR User changes E-mail address at FDR. Use to update information on CSR User card member Profile page Also update card member's profile in Siebel Self-Service for Cards

NOTES:	6. Confirm that if account does not exist in Siebel Self-Service for Cards, it can be assumed to be a new card member account.
	7. For lost & stolen cards, the new account must be linked to all previous accounts so that all previous history is displayed and the history displays the (last four digits) of the corresponding account number.

2.15.7 Upload MSR Data (972)

Name:	**Upload MSR Data**
Brief Description:	System reads the daily statement cycle (MSR) file sent from FDR to update Siebel Self-Service for Cards with statement data.

Main Path:	1. System reads transactions from MSR file:
	   a. For each record, system determines whether an e-mail notification is required and sends e-mail according to rules defined in Send E-mail Notification use case
	   b. For information that is required for presentment of statement information, the system stores information in card member database

Notes:	See data formats in Appendix B – MSR Data Format

MSR Data Format

The MSR data is as defined by the FDR document, "CARDHOLDER STATEMENT TAPE FORMAT (015)" Version "04.1.1 – MAJOR." See Appendix B – MSR File Mapping for a mapping of MSR fields to Siebel Self-Service for Cards statement data.

2.15.8 Upload MON Data (971)

Name:	**Upload MON Data**
Brief Description:	System reads the daily Monetary (MON) file sent from FDR to update Siebel Self-Service for Cards with recent account activity.

Main Path:	1. System reads transactions from MON file:
	   a. For each transaction, system determines whether an e-mail notification is required and sends e-mail according to rules defined in Send E-mail Notification use case:
	     i. Payment Posts To My Account
	     ii. Credit Return Posts To My Account
	     iii. Posted Item Exceeds X$ (Only applies to Debits)
	   b. For information that is required for presentment of Recent Activity information, the system stores information in card member database

Notes:	Siebel needs new FDR 037 file formats (requested on 3/23/04) to finalize these requirements.

MON Data Format

The MON data is as defined by the FDR document, "COMBINED CARDHOLDER MASTER AND FLAP FILE (095)" Version "03.9.4 – MAJOR." See Appendix C – Monetary File Format for a mapping of MSR fields to Siebel Self-Service for Cards statement data.

2.15.9 Send E-mail Notification (930)

Name:	**Send E-Mail Notification**
Brief Description:	System sends an e-mail to notify the card member of a system event (See Appendix A – E-Mail Notifications), for example, that the statement is available, or a card member configured alert has been triggered.
Trigger	System detects an event that should result in an e-mail to the card member
Main Path:	1. System determines that card member requires an e-mail notification [A1] – [A22] 2. System retrieves e-mail address of card member [B1] 3. System sends e-mail message to the SMTP server

Alternate Paths:	**[A1]Secure Message Reply available (real-time):**
	    1. CSR User creates a response to a Secure Message
	    2. System creates a real-time e-mail notification
	
	[A2]Convenience checks ordered (real-time):
	    1. Card Member orders convenience checks
	    2. System creates a real-time e-mail notification
	
	[A3]Card Member profile changed (real-time):
	    1. Card Member changes address, e-mail address, or phone number
	    2. System creates a real-time e-mail notification
	
	[A4]Card Member paper status changed (real-time):
	    1. Card Member turns paper on or off
	    2. System creates a real-time e-mail notification
	
	[A5]New statement is available AND e-mail has not been sent for the current cycle (batch, MSR):
	    1. System creates a batch e-mail notification
	
	[A6]Payment is past due AND enrolled in Siebel Self-Service for Cards (batch, CHD)
	    1. System checks that Current Date is greater than Payment Date and Payment Past Due Alert Flag
	    2. If payment is past due, system creates a notification that includes the payment date, payment date and URL to the QuickPay page
	    3. System creates a batch e-mail notification
	
	[A7]Payment due within x days (batch, CHD, once per statement cycle):
	    1. If Current Date - Payment Due Date < X System creates a batch e-mail notification
	
	[A8]Credit limit is reached (batch, CHD):
	    1. System checks that Current Balance meets or exceeds card

member's Credit Limit

2. If limit is reached and e-mail has not already been sent for this condition, system creates a batch e-mail notification

[A9]Within $X of Credit Limit (batch, CHD, once per statement cycle):

1. If Current Balance - Credit Limit < 0 AND an e-mail has not been sent already for this statement cycle, the system creates a batch e-mail notification

[A10]   Balance exceeds x amount (batch, CHD, once per statement cycle):

1. If Current Balance > X AND an e-mail has not been sent already for this statement cycle, the system creates a batch e-mail notification

[A11]   Balance drops below x amount (batch, CHD):

1. If Current Balance < X AND an e-mail has not been sent already for this condition, the system creates a batch e-mail notification

[A12]   Payment posts to account (batch, MON):

1. System reads MON file
2. System finds payment posted to Account
3. System creates a batch e-mail notification

[A13]   Credit posts to account (batch, MON):

1. System reads MON file
2. System finds credit posted to Account
3. System creates a batch e-mail notification

[A14]   Transaction exceeds x amount (batch, MON):

1. System reads MON file
2. System finds transaction for > $X for Account
3. System creates a batch e-mail notification

[A15]   Card Member enrolls:

1. Card Member submits enrollment information
2. System creates a real-time e-mail notification

[A16]   Payment submitted:

1. System creates a payment record in the payment file
2. System creates a real-time e-mail notification

[A17]   Direct Bill Pay payment made

1. Card Member submits a Direct Bill payment
2. System creates a real-time e-mail notification

[A18]   Suppress Paper Statement request submitted

1. Card Member submits a Suppress Paper request
2. System creates a real-time e-mail notification

[A19]   Card Member Changes Payment Account Information

1. System creates a real-time e-mail notification

[A20]   Payment account information changed (in CHD file):

1. System reads CHD file
2. System finds account changed transaction
   a. System updates card member's payment account information

Business Rules:	[B1] If card member has configured a separate alert e-mail address, send

	the alert notification to that address, otherwise use the card member's profile address. [B2] All system-generated e-mails go to the profile e-mail address. Note: FDR is the system of record, so this is updated during the daily CHD file upload process if the e-mail changes at FDR. [B3] If system event is a change of e-mail address, send a notification to both the old and new e-mail address. [B4] In the event of any update to the card member's profile address, or phone number, the system will send a fraud alert notification to the card members current profile e-mail address.
Exception Paths:	**[E1] No e-mail address for the card member:** System ignores request and does not send any e-mail
Notes:	The following alert notifications (e-mails) are driven off the Credit Limit (CL) and/or Current Balance (CB) received in the daily FDR Change Data file: 1. Credit Limit Reached 2. Balance is Within $X of Credit Limit 3. Balance Exceeds $X 4. Balance Drops Below $X 5. Payment Due in X days The following e-mails are driven off the Monetary (MON) file and should contain a URL that re-directs the card member to Recent Activity page after successfully authentication into Siebel Self-Service for Cards: 1. Payment Posts To My Account 2. Credit Return Posts To My Account (Details for differntiation Credit versus Payment transactions are in the MON file) 3. Posted Item Exceeds X$ (Only applies to Debits) The following e-mails are generated in real-time in response to card member actions 1. Convenience checks ordered 2. Paper turned on or off 3. Address changed 4. E-mail address changed 5. Phone number changed 6. Card Member enrolled (Note that multiple e-mails may be generated for real-time e-mails in the same day) No more than one e-mail will be sent per day per type of e-mail (batch), regardless of number of transactions that meet the criteria in the daily file. (But multiple e-mails will be created for different types of transaction) New Statement Available e-mail is triggered by monthly bill load of the bill data file (MSR file). Personal occasion alert has been removed as a requirement. Spending Threshold alert has been removed as it is covered by Posted item Exceeds or Balance Exceeds alerts. Card Member may enter an e-mail address specifically for alerts. This is defaulted to the primary E-mail Address. If a user updates the Alert e-mail address, the system stores this separately from primary (profile) address as

	a secondary e-mail address to be used for all alerts.
	See Appendix A – E-Mail Notifications for specifications of alert e-mail notifications.

2.15.10 Log User Activity (940)

Name:	**Log User Activity**
Brief Description:	System logs card member and CSR User activity
Trigger:	User performs an activity that triggers a log event

Main Path:	1. System creates a log record including:
	    a. Timestamp
	    b. Account Number
	    c. Action
	    d. Language Indicator
	    e. IP Address
	 2. System records event in the activity table

2.15.11 Create Management Report (950)

Name:	**Create Management Report**
Brief Description:	System creates a management report on request (either by Scheduler or Administrator).
Trigger:	System or Admin requests a management report
Main Path:	1. System reads report parameters for specific report [A1]-[A12] 2. System generates a database query 3. System formats query results 4. System writes report to a file

Notes:	Following Reports are generated (See System Reports in Section 6 for further detail on all Reports):
	   Management Reports
	   1. Card Member Activity Report
	   2. Card Member Profile Change Report
	   3. Daily Payment Report
	   4. Daily Direct Bill Pay Report
	   5. Address Change Report
	   6. Card Member Lockout Report

	7. [CSR User Lockout Report](#)
	8. [Secure Messaging Report](#)
	Security Reports
	1. [CSR User Profile Change Report](#)
	2. [CSR Users Activity Report](#)
	3. [CSR User Role Report](#)
	4. [CSR User Security Violation Report](#)
	System Reports
	1. [Statement Monitor Report](#)
	2. [User Information Report](#)
	3. [System Utilization Report](#)
	Reports will be maintained for 4 months.
	The Activity Report runs Midnight – Midnight. EST is fine. Central may be better.
	The Payment Report runs from 7pm EST – 6:59 pm EST.
	Daily Direct Bill Payment Report runs from 7pm EST – 6:59 pm EST.
	lE-mail failures will be reported

2.15.12 Validate Banking Information (980)

Name:	**Validate Banking Information**
Brief Description:	System calls EPICWare software to validate a pair of DDA and ABA numbers. EPICWare software returns a success or error code and, in some cases, a repaired ABA number.
Trigger:	Card Member enters or updates ABA or DDA number.
Main Path:	**1.** System passes DDA and ABA number to EPICWare software **2.** EPICWare returns results including return codes and possibly a repaired ABA number **3.** System returns repaired ABA number and return codes according to EPICWare rules [B1]
Business Rules:	[B1] If EPICWare code is 1,2, 3, or 4, return EPICWare success code but do not change values of ABA number entered by card member. If EPICWare code is 5,6,7, or 8, use modified ABA number and update Siebel Self-Service for Cards database. If EPICWare code is 9, 10, or 11 return failure code
Notes:	

3

Card Manager Administration (CSR)

3.1 Overview

The Case Management use cases cover the business requirements for allowing CSR Users to manage card members.

CSR Users are assigned a role and are only allowed to perform a function if the role has been configured to include the privilege to perform that function. In General, the ability of CSR Users with different privileges to access to different functions is governed by the tabs, buttons, or links displayed on the page.

This section describes the following use cases:

- **Login – CSR User** - Describes the mechanism whereby an CSR user logs in the CSR application.

- **Handle Card Member Inquiry** - CSR User searches for card member information, views the card member profile and takes action to satisfy a card member request or query.

3.1.1 Log In -- CSR User (1000)

Name:	Log In (CSR User)
Brief Description:	Describes the mechanism whereby an CSR user logs in the CSR application.

Main Path:	1. CSR User selects a link to login to the system
	
	2. System presents a form containing the following:
	   a. Login ID
	   b. Password
	   c. **Actions**: Login
	
	3. CSR User completes the form and selects Login action [A1]
	
	4. System authenticates CSR User and displays the *Access Card Member Profile* page
	
	5. Use case ends

Alternate Paths:	**[A1] CSR User password has expired:**
	1. System redirects CSR User to Change Password page and displays a message that the password has expired.
	[A2] CSR User logs in with temporary password after being locked out:
	1. System invokes **Reset Password** use case

Business Rules:	**[B1]** Password expires in 60 days
	[B2] Landing page for all CSR Users is the Access Card Member Profile page
	[B3] If the CSR User does not have privilege to view the Card Member Profile, the user will land on the same page but with a message asking the user to select page using the navigation bar and with the navigation displaying appropriate tabs that the user has privileges to use.
	[B4] CSR User may not log in with a temporary password but must change it before being allowed access. This is functionally the same as when a CM logs in after being given a temporary password.
	[B5] CSR Users are give access to different pages and functions depending on their privileges.

Notes:	

Field Validation

NAME	DESCRIPTION	VALIDATION
*Login ID	Look up in CSR Manager database	8-12 alphanumeric. Not case sensitive. Must exist.
*Password	Display is masked using asterisks	6-12 alphanumeric. Not case sensitive. Must match value stored in the CSR Manager
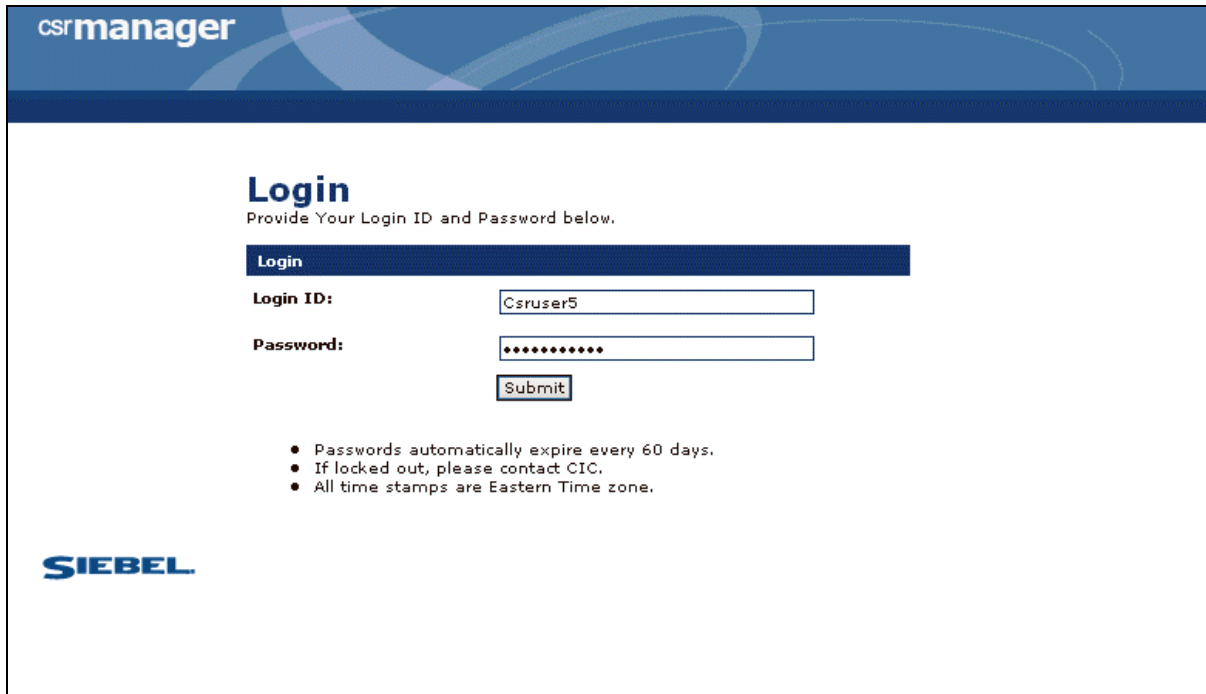
Figure 3.1 – Log In (CSR User)

3.1.2 Handle Card Member Inquiry (1010)

Name:	Handle Card Member Inquiry
Brief Description:	CSR User searches for card member information, views the card member profile and takes action to satisfy a card member request or query.

Main Path:	1. User successfully logs into the system
	2. System displays *Access Card Member Profile* page containing the ability to search on the following: [B5]
	a. Account Number
	b. Social Security Number
	c. Case Number
	d. **Actions**: Authenticate; Clear
	3. CSR User enters full Account Number, OR Social Security Number, OR Case Number and selects *Authenticate* action
	4. System makes ODS call to retrieve card member data:
	a. Primary Name
	b. Paper Off Eligible Flag
	c. Paper Hold Flag
	d. Direct Bill Pay Eligible Flag
	e. Balance Transfer Eligible Flag
	f. External and Internal Status Codes
	g. Social Security Name
	h. Billing Zip Code
	i. Product Code (Brand)
	j. E-mail Address
	5. System displays card member profile information including: [A1] [A2] [B7]
	a. Name
	b. Social Security Number
	c. Account Number
	d. Brand
	e. Enrollment Date
	f. E-mail Address
	g. Billing Zip Code
	h. External Status
	i. Internal Status
	j. Paper Off Status
	k. Enrollment Date/Time Failed [B2]
	l. Enrollment Reason Failed [B2]
	m. Login Name
	n. Date Last Login
	o. Logged In Status
	p. Last Page Accessed
	q. Login Failures [B3]
	r. Date of Last Failure
	s. Reason Failed
	t. List of alerts with alert title and date/time of last notification
	u. List of service qualifications (CC, Add Auth User, Replace Card, Payment Activity, Direct Bill Pay, Paper On/Off)
	v. Access Status (Enabled or Disabled)
	w. Reason for Disabled Access
	x. **Actions**: Unlock CM; Temporary CM PWD; Jump To Page; Login

	As User; Payment History; Enable/Disable Access [B1]
	6. CSR User selects action [A2-A6]

| Alternate Paths: | **[A1] Search on Social Security Number matches multiple Account Numbers:**

1. System displays *Select Account* page showing all accounts matching the Social Security Number:
   a.   List of Accounts (in a dropdown box)
   b.   **Actions**: Authenticate; Back
2. CSR User selects account from the list
3. CSR User selects *Authenticate*
4. Use case continues from Step 3 of Main Path

[A2] CSR User selects *Unlock CM*:

1. System displays a confirmation page:
   a.   Text Message confirming unlocking of the CM user
   b.   **Actions**: Submit; Cancel

2. CSR User confirms unlock by selecting submit action
3. System resets card member's login failure status and enroll fail count to zero

[A3] CSR User selects *Reset CM Password*:

1. System displays the *Reset Password* page:
   a.   Text Message confirming the password reset
   b.   **Actions**: Submit; Cancel
2. CSR User confirms by selecting the submit action
3. System displays a page displaying a randomly generated temporary password, made up of 6 lower case letters and digits **[B4]**
4. System resets the password to the temporary password value
5. System resets card members login and enroll fail count to zero
6. CSR User informs card member of new temporary password

[A4] CSR User selects *Jump To Page*:

1. CSR User clicks *Jump to Page* button.

2. System displays a read-only version of the page that the card member is on, or if the card member is on a series of form entry pages, the system will display the first page of the series. **[B6]**
3. CSR User may view the page, but will not have the ability to perform any actions on the page or navigate to another page

[A5] CSR User selects *Login As Card Member*:

1. CSR User clicks *Login as Card Member* button.
2. System displays card member application *Account Summary* page
3. CSR User may navigate card member application and perform actions as if they were the card member.
4. CSR User selects a tab to navigate back to CSR User functions |

Alternate Paths:	**[A6] CSR User selects *Payment History*:**
	1. System displays Payment History module from card member's *Payment History* page with all links disabled
	2. CSR User views card member's billing and payment transactions, but is unable to make any changes to card member information
	[A7] CSR User selects *Enable/Disable Card Member Access*:
	1. System displays the *Enable/Disable* page: [B8]
	a. Text Message confirming the enabling/disabling
	b. Reason
	c. **Actions**: Disable Access; Clear; Cancel
	2. CSR User enters reason and confirms disabling by selecting Disable Access action
	3. System toggles the card member status and redisplays the card member Profile page with a success message:
	a. Disable Access action: "Successfully disabled the card member"
	b. Enable Access action: "Successfully enabled the card member"
	[A8] CSR User selects *Case History*:
	1. System Displays *Case History* Page including: [B5]
	a. Case Number
	b. Opened (Date/Time)
	c. Category
	d. Owner
	e. Status (Open; Answered)
	2. CSR User selects case
	3. System displays *Case Detail* page
Exception Paths:	**[E1] Card Member not found:**
	System displays the input form containing previously entered fields and a message indicating that card member was not found
Business Rules:	**[B1]** CSR Users will be able to perform actions depending on the privileges they have been granted, which is dependent on the role they have been assigned. If the CSR User does not have a privilege, the system will not display the feature (in this case a button) that allows the user to perform the action.
	[B2] The system will not display the module of enrollment failures if there are no failures. (Reasons for enrollment failure are CVV mismatch, SSN mismatch, Account Number mismatch, Name mismatch, E-mail mismatch, ZIP mismatch)
	[B3] Reasons for login failures will be displayed on the same line. (There are two possible reasons, either invalid password or invalid secret answer)
	[B4] For password reset, the system generates a random password. The card member must change the password the next time he or she logs in.
	[B5] The system logs actions taken by a CSR User as defined in the

Activity Log report use case

[B6] Jump to Page will display the last page recorded in the activity log, only if the card member is still logged in. It will also log the specific statement date that a card member has viewed

[B7] If CSR User selects Profile after performing an action, the System will display the current profile.

Notes:	
	Jump To Page displays the Last Page that the user was on at the time the card member Profile was displayed, but the data on the page is not displayed and error messages on the page are not displayed, because the system is displaying a fresh page and form data is either in the card member's browser or session data. The Last Page will be the title of the Page (as displayed in the card member's URL for the page). In cases where multiple pages have the same name, the Last Page Accessed will not uniquely specify the page, but will specify a set of related pages, (e.g., data entry, confirmation pages)
	Card Member information will be obtained from the billing system using ODS calls as needed. (See ODS Calls By Feature).
	Siebel Self-Service for Cards will capture card member's SSN at login so that each card member has an associated SSN and the system can search for card member accounts by SSN.
	All failures will be displayed until the card member logs in successfully or CSR User resets them.
	CSR Users need to see a card member's eligibility for services. These will be listed under Service Qualifications (See business rules for Order Services use case for qualification): Convenience Checks/Replacement Card/Add Auth (Qualify/Does Not Qualify) Direct Bill Pay (Qualify/Does Not Qualify) Paper Suppression Eligible/Paper Status (Qualify/Does Not Qualify, Yes/No,) Payment Activity (Yes/Blank).
	Enrollment and Login failure details are obtained from activity logging tables.
	The list of alerts are obtained from the notification profile that is maintained through the Manage Notifications use case. Credit limit reached

	Statement available Payment due Balance within Balance exceeds Balance drops below Payment posts Credit posts Transaction exceeds
	The Payment Activity will be set to Yes if any online payments have been made to the account at any time (so that there are entries on the payment history page). Card Member History will display date and time to be consistent with other timestamps displayed by the CSR User application. The system will display different tabs, buttons and links depending on the CSR User's privileges, See the table below and Appendix I, CSR User Access Rules for further details. If an CSR User is impersonating the user and the user is a "first-time user," then the CSR User will be taken directly to Account Overview screen, by-passing normal card member enrollment steps. The card member will then need to enroll as first-time user when he/she first logs in.

Privileges

PRIVILEGE	DESCRIPTION	SYSTEM ACTION
View Card Member Profile	May view card member billing and payment information but may not make changes to card member information	Show *Card Member* tab. Show *Payment History* button
Accept, Return and Escalate Case	May view card member case history	Show Case History subtab.
Jump To Page	May view the page that the card member is on, but not make any changes to card member information.	Show *Jump to Page* button
Enable/Disable Card Member Access	May disable or enable a card member account	Show *Enable Access OR Disable Access* button. Display current status.
Reset Card Member Password	May reset a card member password	Show *Reset CM PWD* button
View Payment History	May view card members case history, but may not update card member	Show *Payment History* button
Unlock CM	May unlock card member setting login and enrollment count to zero and allowing card member to try logging in again	Show *Unlock CM* button
Login As Card Member	May access Siebel Self-Service for Cards application as the card member and make any changes to the card member account	Show *Login As User* button.

Figure 3.2 – Access Card Member Profile – Authenticate Customer
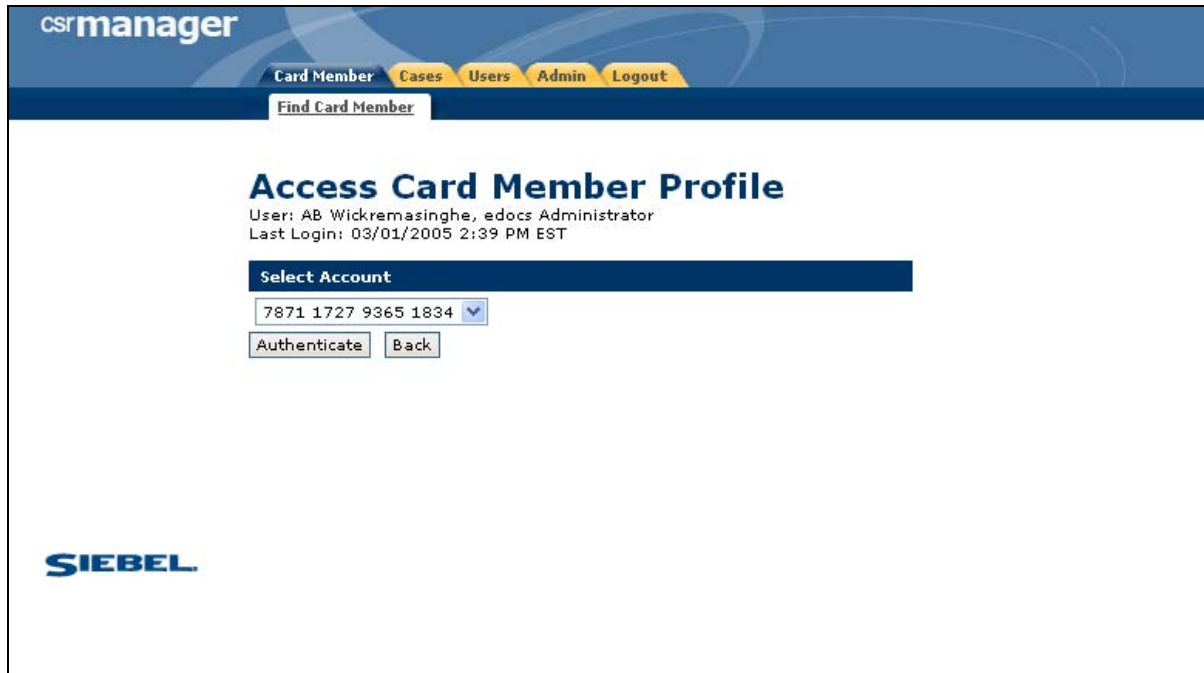
Figure 3.3 – Access Card Member Profile – Select Account

Figure 3.4 – Card Member Profile

csr**manager**

Card Member | Cases | Users | Admin | Logout

Find Card Member

Case History
User: AB Wickremasinghe, edocs Administrator
Last Login: 02/28/2005 3:13 PM EST

Card Member Profile   Case History

You are not authorized to view one or more of the cases returned by this search.

List Of Cases

Case No.	Opened	Category	Owner	Status
102001	10/27/2004 05:52PM	Account Status	Albert, Lev	Closed
1000001	11/11/2004 01:35PM	Account Balance	Albert, Lev	Open
1000002	11/12/2004 11:26AM	Dispute Transaction	Albert, Lev	Open
1000003	11/15/2004 12:08PM	Account Balance	Yedla, Usha	Closed
1000004	11/15/2004 12:08PM	Dispute Transaction	Albert, Lev	Open
1000009	11/30/2004 06:14PM	Dispute Transaction	Albert, Lev	Open
1000010	11/30/2004 06:16PM	Dispute Transaction	Albert, Lev	Open
1000014	11/30/2004 06:34PM	Dispute Transaction	Albert, Lev	Open
1000015	11/30/2004 06:38PM	Dispute Transaction	Albert, Lev	Open
1000041	02/01/2005 11:34PM	Account Balance	CSR Case Queue	Closed
1000045	02/13/2005 02:46AM	Dispute Transaction	CSR Case Queue	Open
1000047	02/16/2005 08:06PM	Dispute Transaction	CSR Case Queue	Open
1000048	02/18/2005 02:04AM	Account Balance	CSR Case Queue	Open
1000049	02/28/2005 02:59PM	Account Status	CSR Case Queue	Open

Figure 3.5 – Case History

Figure 3.6 – Unlock Card Member

Figure 3.7 – Unlock Card Member Success
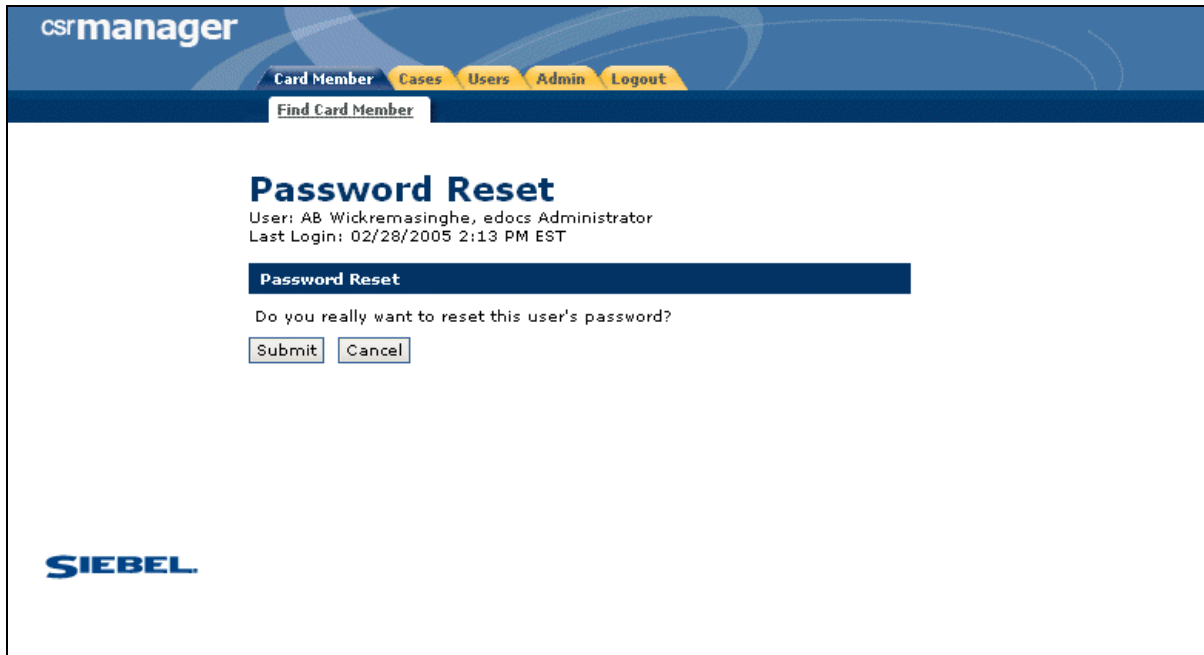
Figure 3.8 – Reset Password
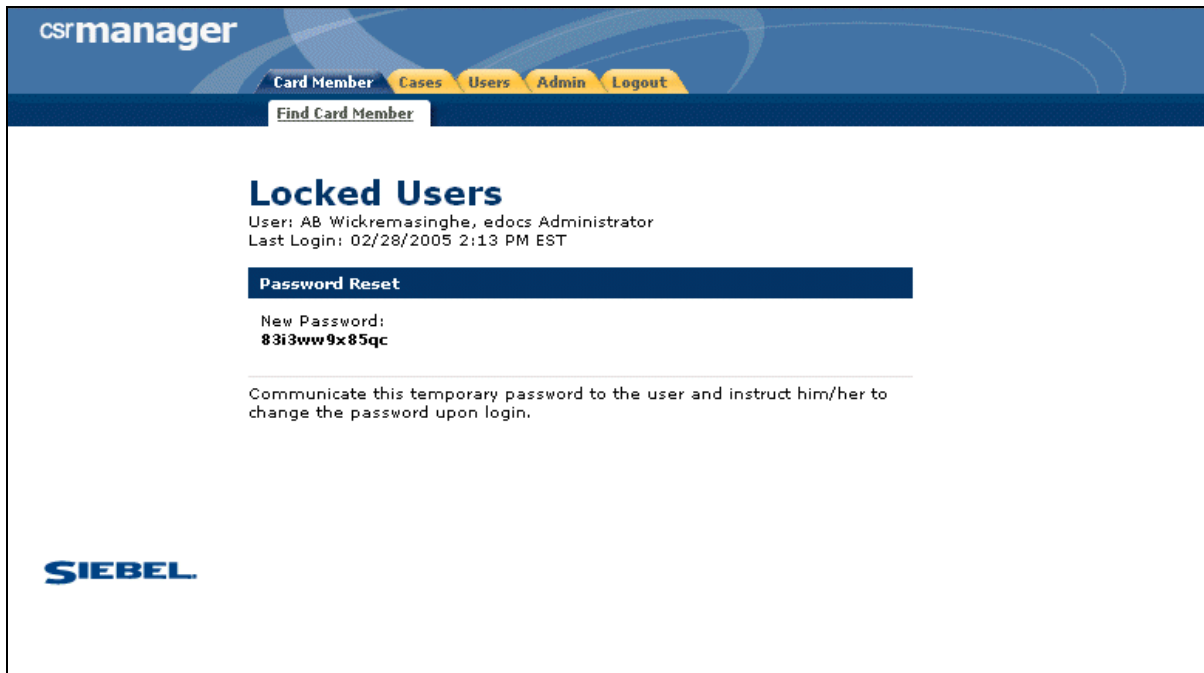
Figure 3.9 – Reset Password Success

Figure 3.10 – Payment History
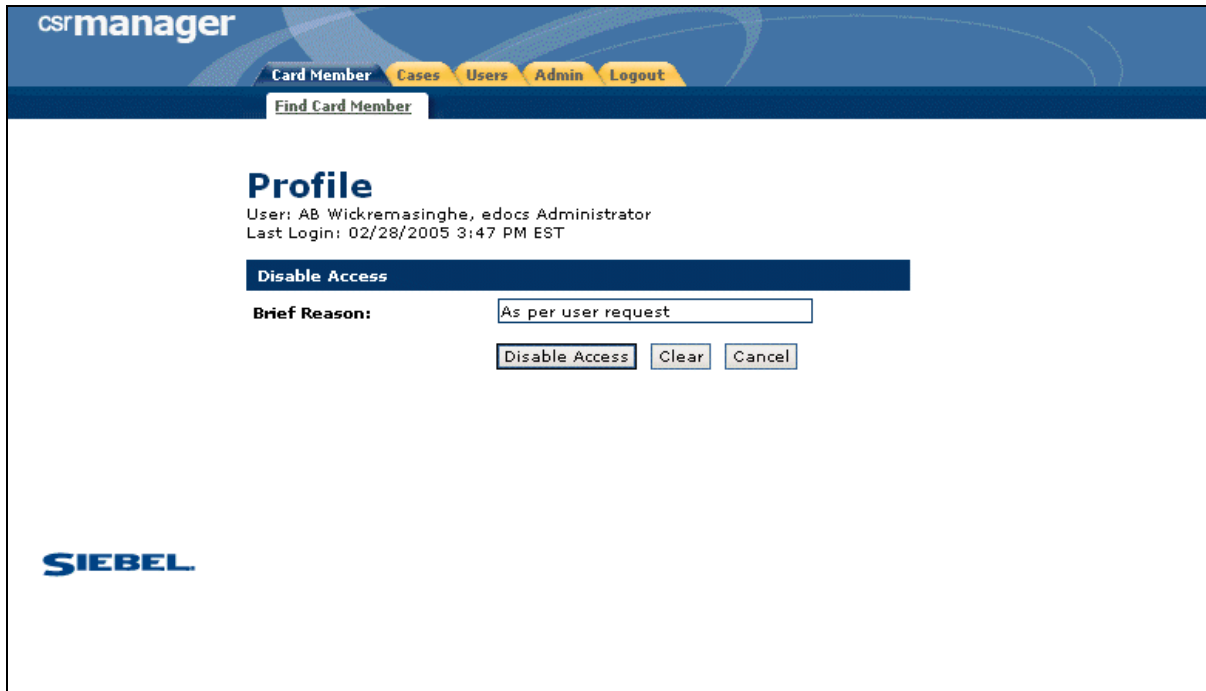
Figure 3.11 – Disable Access

Figure 3.12 – Disable Access Success

Figure 3.13 – Enable Access

3.2 Case Management Use Cases

The Case Management use cases describe the business requirements for allowing CSR Users to retrieve, reply to and manage all online cases.

3.2.1 Respond to a Case (1020)
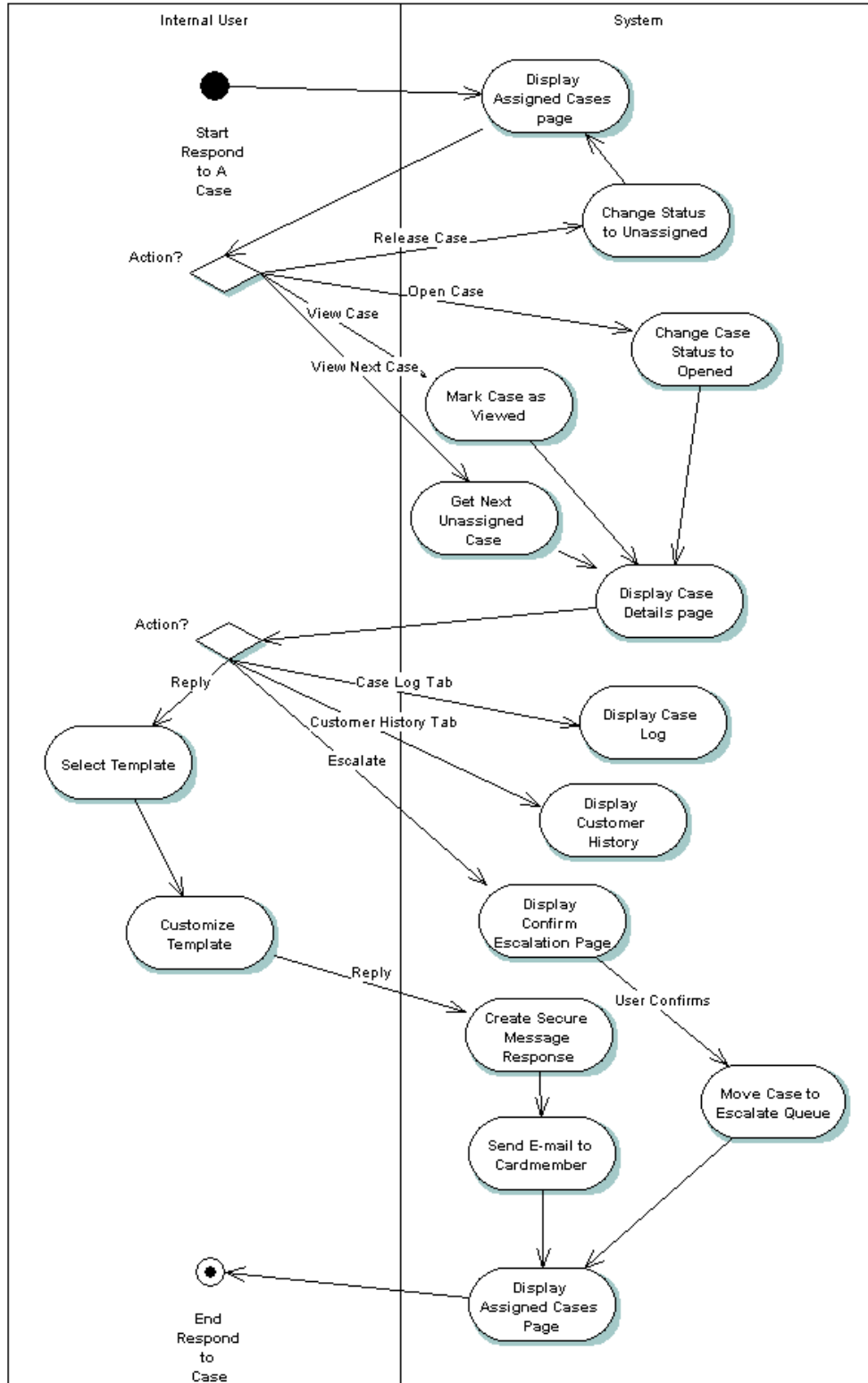
Figure 3.14 – Activity Diagram For Respond To A Case

Name:	**Respond to a Case**
Brief Description:	CSR User retrieves a case from a work list and submits a response to a card member.

Main Path:	1. CSR User navigates to Cases tab and *Assigned Cases* sub tab [A1] [B1]
	
	 2. System displays *Assigned Cases* page containing the following columns:
	    a. Checkbox
	    b. Case No. (hyperlink)
	    c. Created (Date/Time)
	    d. Last Updated (Date/Time)
	    e. Card Member Name
	    f. Category
	    g. Subject
	    h. **Actions:** Release Selected; Release All
	
	 3. CSR User selects the Case Number of the case to work on [A2] [A3]
	
	 4. System displays *Case Details* page for selected case, containing the tabs:
	    a. Case Details
	    b. **Actions**: Change [Category]
	    c. Case History
	    d. Case Log
	    e. As well as case context information:
	    f. Case Number
	    g. Card Member [Name]
	    h. Account Number
	    i. Category [dropdown box]
	    j. Status
	    k. Created [Date/Time]
	    l. Opened [Date/Time]
	    m. Updated [Date/Time]
	    n. CSR User ID
	    o. Case Content [Full text of case (including previous messages in reverse chronological order similar to Card Member Case Detail)]
	    p. Notes and Replies form containing the following fields:
	    q. Language [radio button] (Default to CM's language)
	    r. Categories: [dropdown box] List of available sub-categories
	    s. Template Category: [dropdown box] List of available response templates (for given sub-category)
	    t. Content: Text box to enter Response
	    u. **Actions**: Paste; Reply/Close; Clear; Escalate; Cancel
	
	 5. CSR User selects a sub-category to answer the case [A4][A5][A6] [A11]
	
	 6. System populates list of templates for this sub-category in the template dropdown menu.
	
	 7. CSR User selects a template and clicks *Paste*.
	
	 8. System populates the text box

	9. CSR User completes form and selects *Reply/Close* respond to case. [A6] [A10] [B8]
	10. System updates secure message status and stores secure message
	11. System creates a notification e-mail (unsecured) containing a standard e-mail template with a link to the Secure Message Inbox page and sends it to the card member
	12. System redirects CSR User to *Assigned Cases* page
Alternate Path	**[A1] CSR User selects Search Cases:**
	1. System displays the *Search Cases* page: **[A4][B4]**
	a. Case No. [checkbox; text field]
	b. Account No. [check box; text field]
	c. Age of Case [checkbox; dropdown box: 0-6; 7-12; 13-24; 25-48, 49-72, >72)]
	d. Category [check box; dropdown box]
	e. Assigned/Not Assigned [checkbox; radio button: Not Assigned/Assigned Owner selection dropdown]
	f. Queue: [checkbox; dropdown box: Escalated/Not Escalated]
	g. Date Created [checkbox; (From Date) (To Date) fields]
	h. Last Date Updated [checkbox; (From Date) (To Date) fields]
	i. **Actions**: Search; Clear
	2. CSR User selects search criteria and selects submit action
	3. System displays search details with results set including:
	a. Search Details (criteria form)
	b. Case No. (hyperlink)
	c. Created (Date/Time)
	d. Last Updated Date/Time
	e. Card Member Name
	f. Category
	g. Subject (Case)
	h. **Actions**: Accept Selected; Assign Selected; Link on case number
	4. CSR User selects link on case number [A7] [A8] [A12]
	5. System displays Case Detail page with no reply box (view only): [B9]
	a. Case detail tabs
	b. Case detail header
	c. Case content
	d. **Actions**: Accept; Back
	[A2] CSR User Releases Cases:
	1. CSR User selects one or more cases on the list of assigned cases and selects Release Selected action
	2. System changes status of the selected cases to unassigned
	3. System redisplays list of cases showing only assigned cases
	[A3] CSR User selects *Accept Next Case*:
	1. System selects the next unassigned case that the CSR User can

work on and assigns it to the CSR User

2. System changes the status of the case so that other CSR Users cannot work on it

3. System redirects the CSR User to the Case Detail page and displays details of the case

[A4] CSR User selects *Card Member History*

1. System displays *Case History* page including:
   a. Case context information (same fields as Case Detail)
      List of cases for this card member including:
   b. Case No. (hyperlink)
   c. Opened (Date/Time)
   d. Category
   e. Owner)
   f. Status

[A5] CSR User selects *Case Log*

1. System displays *Case Log* page including:
   a. Case context information (same fields as Case Detail)
      Log Content for this card member including:
   b. Update Date/Time
   c. CSR
   d. Action Type
   e. Note/Reply (Hyperlink to full text based on beginning of text)
2. CSR User continues by navigating to another page using tabs and sub-tabs

[A6] CSR User selects Escalate [B4]

1. System displays *Confirm Escalation* page:
   a. Case context information (same fields as Case Detail)
   b. Text message ("Are you sure you want to escalate?")
   c. Text box to enter note
   d. **Actions**: Escalate; Cancel
2. CSR User selects escalate action with or without entering note
3. System moves case to the escalation queue
4. System redirects user to *Assigned Cases* page

[A7] CSR User (with sufficient privileges) re-assigns case to different CSR User [B3]

1. CSR User (with Assign Case privilege) selects one or more cases from list of cases
2. CSR User selects *Assign Selected* action
3. System displays Assign To User page including table of users for this CSR User containing:
   a. User ID
   b. Role
   c. Number of Cases
   d. **Actions**: Assign; Cancel
4. CSR User selects user and assigns to case
5. System redisplays the page containing:
   a. Same information as before
   b. **Actions**: Submit; Cancel

	6. CSR User confirms
	7. System changes ownership of case
	8. System takes CSR User back to search page.
	[A8] CSR User edits the response template before sending
	1. CSR User adds to or edits the response template after it has been selected and populated in the text box.
	2. Use case continues from Main Path Step 10
	[A9] CSR User Changes Category:
	1. CSR User selects a category from the drop-down menu [B7]
	2. System changes the category for the case
	3. System redisplays Case Detail page with the changed category [A13]
	[A10] CSR User accepts one or more cases from search results:
	1. CSR User selects one or more cases from the list of case
	2. CSR User selects Accept Cases action
	3. System puts selected cases on the CSR User's queue and changes status to "Accepted"
	[A11] CSR User changes category to another category to which the CSR User does not have access:
	1. System releases case back to the general queue
	2. System redirects CSR User to *Search Cases* page
Business Rules:	**[B1]** Once an CSR User accepts a case, the case is "locked" and cannot be edited by any other CSR User.
	[B2] The *Search Cases* results page will be sorted to display the oldest cases at the top of the list (First in First out).
	[B3] *Assign Selected* is only available to an CSR User with Assign Case privilege. Other CSR Users cannot see this button and can only accept cases, release them back to the queue or escalate them to the escalated queue.
	[B4] CSR Users are not required to add a note when escalating.
	[B5] The CSR User activity report will log each case that has been viewed.
	[B6] The case category can only be changed by the owner of the case when the case is open
	[B7] The CSR User may not select the *Reply & Close* action without selecting a template
	[B8] If the CSR User selects a case from the Search page, the Accept Button will only be displayed if the case is not Accepted
Notes:	Time created is the time the case was opened by the card member. Time last updated is the time case was closed or updated by an CSR User.
	The case list could be a scrolling list (up to about 200 cases) or paging. If it uses paging, it should display 30 cases to a page.
	The system will display different tabs, buttons and links depending on the CSR User's privileges.
	The Assign Selected button is only active when the CSR User has selected a category in the Search Cases screen and all the selected

cases are for the same category.

CSR User name on the display should be displayed in format First Name Last Name, e.g., "Adam Smith"

If an CSR User enters any text in the content area before selecting *Change Category*, this text will be ignored

The list of users that an CSR User can select from on the *Search Cases* page will only include CSR Users whose profile includes one or more of the categories assigned to the CSR User performing the action. This also applies when the CSR User selects the *Assign Selected* button from the search results.

See list of categories. Note that the sub category name and template name for Dispute Transaction will be Miscellaneous and Blank Template respectively.

If the Assigned/Not Assigned checkbox is not selected, the results will include cases that are both accepted and not accepted

The status and sub-status corresponding to different actions are: Created - Open / Unassigned; Accepted - Open / In Progress; Released - Open / Unassigned; Escalated - Open / Unassigned; Assigned- Open / In Progress; Replied - Closed / Replied; Reopened - Open / Unassigned; Changed Category - Open / In Progress or Open / Unassigned; Closed - Open / Deleted By CardMember

If no user is selected from the pull-down menu then all users assigned users will be returned.

If the CSR User selects search by case number and the search is successful, the system should redirect the user to the Case Details page with the result.

Truncate subject (to maximum length that fits, about 20 characters followed by space and three periods) if subject is too long to display on one line

Privileges

PRIVILEGE	DESCRIPTION	SYSTEM ACTION
Accept, Return and Escalate Case	CSR Users with this privilege may reply to cases that they have taken off the queue, and may also return them to the queue or escalate them to an escalated queue.	Show *Cases* tab. Show all buttons except *Assign Selected* and *Mark Case as Viewed*
Assign Case	Supervisors and other managers may assign or re-assign any cases for categories to which they have access rights to a member of any of those categories.	Show *Assign Selected* button Show list of users belonging to the list of categories to which the user has access.

Figure 3.15 – Assigned Cases

Figure 3.16 – Release Selected Assigned Cases

Figure 3.17 – Search Cases

Figure 3.18 – Search Case Results

Figure 3.19 – Case Detail

Figure 3.20 – Confirm Escalation

Figure 3.21 – Card Member History

Figure 3.22 – Case Log

3.3 CSR User Administration Use Cases

The CSR User administration use cases cover the business requirements for allowing CSR User administrators to manage the system including adding CSR Users, managing privileges, and managing templates.

As for other CSR User use cases, some actions will only be available to CSR Users with privileges to perform those actions.

3.3.1 Change Password (1030)

Name:	**Change Password**
Brief Description:	CSR User changes his or her own password

Main Path:	1. CSR User navigates to Admin tab and Change Password sub tab
	
	2. System displays *Change Password* page including entry fields for:
	  a. Current Password
	  b. New Password
	  c. Confirm New Password
	  d. Actions: Submit; Cancel
	
	3. CSR User enters information and selects Submit action
	
	4. System changes the password and displays a confirmation page
	
	5. CSR User selects continue action
	
	6. System displays Access Card Member Profile page

Exception Paths:	**[E1]CSR User enters invalid form entry field or password:** 1. System displays the input form containing previously entered fields with the entered characters replaced by "*" and a message indicating that one or more of the entered values was invalid
Notes:	Allowed values of passwords and rules for validation are the same as Card Member application. Passwords expire after 60 days. Enhancement request: System should track last six passwords and not allow them to be reused.

Form Validation

NAME	DESCRIPTION	VALIDATION
*Old Password	Display is masked using asterisks	Old Password matches password in database
*New Password	Created by card member. Display is masked using asterisks	6-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive. Should not match any of previous 6 passwords
*Confirm Password	Display is masked using asterisks	Matches New Password

Figure 3.23 – Change Password

Figure 3.24 – Change Password Success

3.3.2 Manage CSR Users (1040)

Name:	Manage CSR Users

Brief Description:	An Administrator adds, modifies or inactivates CSR Users by assigning them to roles with categories and privileges so that they can perform their assigned work.

Main Path:	**1.** System displays *Manage Users* page with *Find User* module including:
	  a. Last Name
	  b. **Action**: Search
	
	2. CSR User enters Last Name or partial last name with wild card character ("*")
	
	3. CSR User selects *Search* action
	
	4. System displays *Manage Users* page with *List of Users* module including list of users matching the search criteria (case-insensitive) including:
	  a. CSR User Name (Last Name, First Name)
	  b. User ID
	  c. Last Login (Date)
	  d. Role
	  e. Status (Active/Inactive/Locked/Expired)
	  f. **Actions**: New CSR; Edit CSR; Delete CSR; Reset PW; Link to Edit User (on CSR User Name);
	
	5. CSR User selects new user option: [A1] [A2] [A3] [A4] [A5]
	
	6. System displays New User page including entry fields for:
	  v. Roles (Dropdown: list of roles)
	  First Name
	  Last Name
	  Locations (Dropdown: White Marsh, Jacksonville, Orlando, Tulsa, Minnetonka, Duluth, Scottsdale)
	  Login ID
	  New Password (Blank)
	  Confirm Password
	  Assigned Categories (Checkbox: list of all secure message categories)
	  Escalated Queue (checkbox)
	  Actions:Submit; Clear; Cancel
	
	7. CSR User enters information, selects a single role, one or more categories for the CSR User, selects access to escalate queue and selects Submit action.
	
	8. System displays the *Manage User*s page listing all CSR Users in categories accessible by CSR User and includes the newly added CSR User. **[B2]**

Alternate Paths:	**[A1] CSR User (with sufficient privileges) selects user from the list and Edit User OR selects link on CSR User Name:**
	  1. System displays *Edit User* page with the same fields as New User page pre-populated with previously registered information for the user
	  2. CSR User updates fields and selects submit action
	  3. System updates profile for the selected user
	  4. System redisplays the List of Users page
	
	[A2] CSR User (with sufficient privileges) selects Delete User:

	1. System displays Delete User page including:
	   a. Role
	   b. Name
	   c. **Actions**: Delete; Cancel
	2. CSR User selects Delete action
	3. System logs details of inactivated user and disables the user's access
	4. System displays list with CSR User status updated
	
	[A3] CSR User (with sufficient privileges) selects link to Role:
	1. System redirects CSR User to *Edit Role* page. See *Manage Roles* Use Case
	
	[A4] Search criteria matches more than 50 CSR Users:
	1. System redisplays page with an error message stating that search returned too many users and asking user to refine the search criteria
	
	[A5] CSR User (with sufficient privileges) selects user from the list and Reset PW. See *Manage Locked Users* Use Case:
	1. System displays Reset Password page including:
	   a. User Name
	   b. Message: "Do you really want to reset is user's password?"
	   c. **Actions:** Reset, Cancel
	2. CSR User selects *Reset* action
	3. System sets CSR User password to a temporary password and resets login failure count
	4. System logs CSR User activity
	5. System displays *Password Reset* confirmation page including: [B2]
	   a. Temporary password
	   b. **Actions**: Back
	6. CSR User selects *Back*
	7. System redirects user back to *Manage Users* page

Business Rules:	**[B1]** The system will display a maximum of 50 users in the list of users. If the search criteria matches more than 50 users, the system will display a message asking the user to narrow the search criteria. **[B2]** CSR Users are enrolled as users of the system in the same way as card members, but the system will not allow them to use card member functions. Also, the CSR User may NOT enroll separately with the same Login ID in the card member application. **[B3]** Manage CSR Users function will only be available to CSR Users and they will be able to perform actions depending on the privileges they have been granted, which is dependent on the role they have been assigned. If the CSR User does not have a privilege, the system will not display the feature (or in this case the entire tab) that allows them to perform the action. **[B4]** Any manager can manage any CSR User with *Accept, Return and Escalate Case* privilege. **[B5]** For password reset (on unlock), the system generates a random password. The CSR User is prompted to change the password immediately after their next login. **[B6]** An Administrator will only be allowed to delete one CSR User at a time.

Notes:	The page will display the results module only after a search has been initiated. When the CSR User first comes to the page the results module will not be displayed.
	The names will be displayed as Last Name, First Name (e.g., Smith, Adam).
	Cancel will return the CSR User to the List of Users page with Search field cleared, but previous list of users.
	Any manager can manage any CSR User CSR User with Accept, Return and Escalate Case privilege (otherwise the system would need to restrict groups of these CSR Users so they are not managed by multiple managers OR it would need to provide the capability to assign CSR Users to a specific manager).
	The system will display different tabs, buttons and links depending on the CSR User's privileges.See the Privileges table below
	The search will be case-insensitive.
	CSR Users will enter only fields that are changed. Fields that are not entered will not be changed. Password is displayed as blank and is not a required field and should only be entered in order to change the password.

Privileges

PRIVILEGE	DESCRIPTION	SYSTEM ACTION
View Roles	May view roles and privileges.	Show *Manage Users* tab. Do not display *Add User* and *Delete User, Edit User,* Show only users in categories to which logged on user has access.
Add/Change/Delete User	Info Security Reps manage security. They may add or delete CSR Users, assign them roles and categories, and reset passwords. Users without this privilege will not see Add User, Delete User, or Edit User buttons	Show *Manage Users* tab and all buttons. Show All users

Field Validation (Create User)

NAME	DESCRIPTION	VALIDATION
First Name	First name (Not titles or initials)	Alphanumeric. Max Length 20. No special characters other than hyphen, apostrophe, or space
Last Name	Last name with no suffixes	Alphanumeric. Max Length 20. No special characters other than hyphen, apostrophe, or space
Login ID	Look up in Siebel Self-Service	8-12 alphanumeric, minimum 1 letter,

	for Cards and CSR User database	1 number. Not case sensitive. Must be unique in the system
New Password	Display is masked using asterisks	6-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive.
Confirm Password	Display is masked using asterisks	6-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive.

Field Validation (Edit User)

As for Create User except fields are not required. Only fields that are changed are validated.

NAME	DESCRIPTION	VALIDATION
Login ID	Look up in Siebel Self-Service for Cards and CSR User database	Must exist. Not editable
New Password	Initially blank. Display is masked using asterisks as user types.	6-12 alphanumeric, minimum 1 letter, 1 number. Not case sensitive.
Confirm Password	Display is masked using asterisks	Must match Password

Figure 3.25 – Manage Users

Figure 3.26 – Create New User

Figure 3.27 – Create New User Success

Figure 3.28 – Edit Users

Figure 3.29 – Delete Users

3.3.3 Manage Locked Users (1041)

Name:	Manage Locked Users
Brief Description:	An Administrator unlocks CSR Users or resets CSR User passwords
Main Path:	1. System displays a *Locked Users* page with *Find User* module including: a. Last Name b. **Action**: Search 2. CSR User enters Last Name or partial last name with wild card character ("*") 3. CSR User selects *Search* 4. System displays *Manage Users* page with *List of Users* module including list of users matching the search criteria (case-insensitive) including [A2]: a. CSR User Name (Last Name, First Name) b. Login ID c. Last Login (Date) d. Role e. **Actions**: Link to Unlock User (on CSR User Name) 5. CSR User selects link on CSR User Name: 6. System displays *Unlock User* page including entry fields for: w. CSR User Name

	Actions: Unlock; Reset PW; Cancel
	7. CSR User selects Unlock [A1]
	8. System resets login failure count to zero
	9. System redirects user back to *Locked Users* page

Alternate Paths:	**[A1] CSR User (with sufficient privileges) selects Reset PW:**
	    1. System displays Reset Password page including:
	        a. User Name
	        b. Message; "Do you really want to reset this user's password?"
	        c. **Actions:** Reset, Cancel
	    2. CSR User selects *Reset*
	    3. System sets CSR User password to a temporary password and resets login failure count
	    4. System logs CSR User activity
	    5. System displays *Password Reset* confirmation page including: [B2]
	        a. Temporary password
	        b. **Actions**: Back
	    6. CSR User selects *Back*
	    7. System redirects user back to *Locked Users* page
	
	[A2] Search criteria matches more than 50 CSR Users:
	    1. System redisplays page with an error message stating that search returned too many users and asking user to refine the search criteria.

Business Rules:	**[B1]** If the search criteria matches more than 50 users, the system will be display a message asking the user to narrow the search criteria **[B2]** For password reset, the system generates a random password. The CSR User is prompted to change the password immediately after their next login.
Notes:	The page will display the results module only after a search has been initiated. When the CSR User first comes to the page the results module will not be displayed. The names will be displayed as Last Name, First Name (e.g., Smith, Adam). Cancel will return the CSR User to the List of Users page with Search field cleared andprevious list of users. The system will display different tabs, buttons and links depending on the CSR User's privileges, See the Privileges table below and Appendix I, CSR User Access Rules for further details. The search will be case-insensitive.

Privileges

PRIVILEGE	DESCRIPTION	SYSTEM ACTION
Reset CSR User Password	Info Security Reps are allowed to unlock users and reset passwords when CSR Users lock themselves out.	Show *Manage Locked Users* tab. Show list of locked users. Show links on user names that link to *Unlock User* page.

		Show all locked users.

Figure 3.30 – Manage Locked Users

Figure 3.31 – Unlock User

Figure 3.32 – Unlock User Success
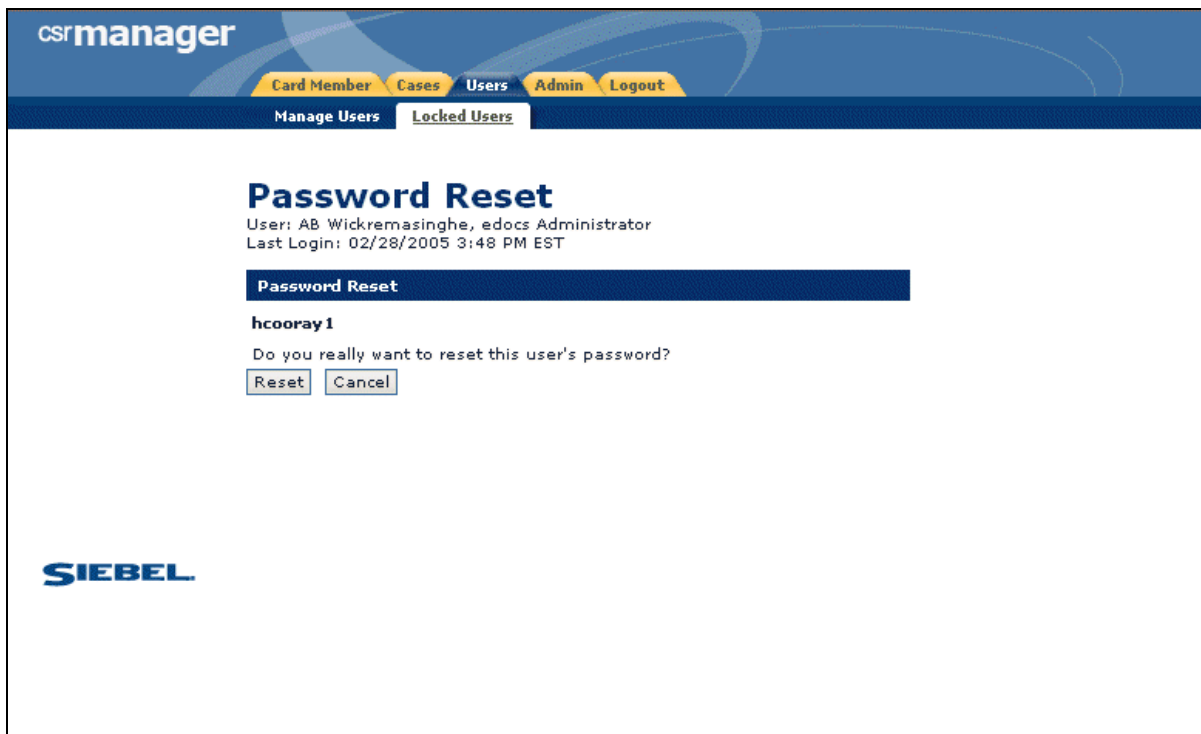
Figure 3.33 – Password Reset
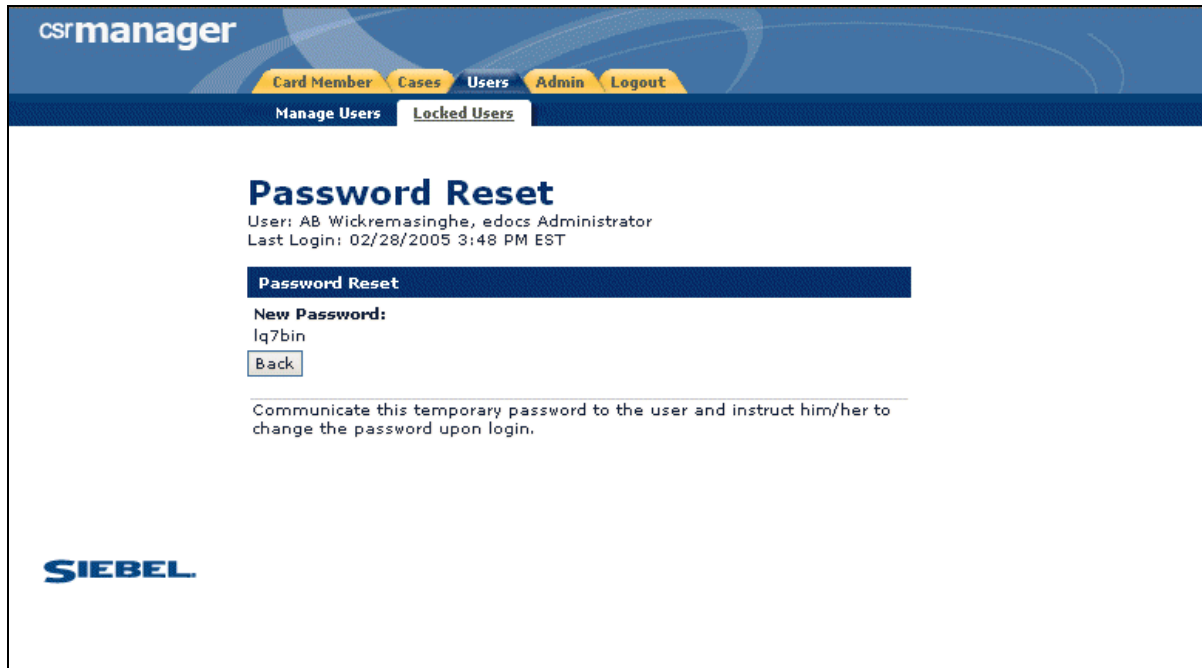
Figure 3.34 –Password Reset Success – New Password

3.3.4 Manage Roles (1050)

Name:	Manage Roles
Brief Description:	CSR User (with sufficient privileges) views, creates and updates roles

Main Path:	1. System displays *Roles* page including:
	   a. Name (Role)
	   b. Assigned Privileges
	   c. Number of CSR Users (within each role)
	   d. **Actions**: New Role ; Edit Role; Delete Role
	
	2. CSR User selects *New Role* [A1]
	
	3. System displays *Create New Role* form including fields for:
	   a. Role Name
	   b. Description
	   c. Privileges (Checkbox: list of privileges)
	   d. **Actions**: Submit; Clear; Cancel
	
	4. CSR User enters role name, selects a set of privileges and selects *Submit* action
	
	5. System creates a new role
	
	6. System creates a record in the activity log
	
	7. System redisplays the *Roles* page showing the list of roles including the newly created role

Alternate Paths:	**[A1] CSR User (with sufficient privileges) selects option to edit an existing role:**
	2. System displays Edit Role page including:
	a. Role Name (non-editable)
	b. Description
	c. Privileges (List : pre-populated with current selections)
	d. **Actions**: Submit; Clear; Cancel
	3. CSR User changes privileges for the existing role and submits [A2]
	4. System stores the updated privileges
	5. System creates a record in the activity log
	6. System redirects CSR User to the Roles page
	[A2] CSR User (with sufficient privileges) selects option to delete an existing role:
	1. System displays Delete Role page including:
	a. Name
	b. Description
	c. Actions: Delete Role; Cancel
	2. CSR User selects *Delete* action
	3. System deletes the selected role
	4. System displays the updated List of Roles
Business Rules	**[B1]** A user may have only one role.
	[B2] The Add/Edit/Delete Roles functionality will only be available to CSR User's that have the *View Roles* privilege. Others will not even see the *Roles* tab.
Notes	The system will display different tabs, buttons and links depending on the CSR User's privileges, See the Privileges table below for further details.

Form Validation

NAME	DESCRIPTION	VALIDATION
*****Role Name**	Title for role	Alphanumeric. Max length=30 characters
*****Description**	Text description of role	Max length=30 characters

Privileges

PRIVILEGE	DESCRIPTION	SYSTEM ACTION
View Roles	May view roles and privileges.	Show *Roles* sub-tab. Do not display *New Role, Edit Role,* or *Delete Role*. Show only users in categories to which logged on user has access.
Update Roles	Info Security Reps manage	Show *Roles* sub-tab. Display

	security. They may add or delete roles. Users without this privilege will not see New Role, Edit Role, or Delete buttons	*New Role, Edit Role,* or *Delete Role*. . Show All Roles

Figure 3.35 – List of Roles

Figure 3.36 – Create New Role

Figure 3.37 – Edit Role

Figure 3.38 – Delete Role

3.3.5 Manage Templates (1060)

Name:	Manage Templates
Brief Description:	CSR User (with sufficient privileges) manages templates

Main Path:	1. System displays *List of Templates* page including:
	  a. Name
	  b. Language (English or Spanish; Default is English)
	  c. Category
	  d. Subcategory
	  e. Status
	  f. Actions: New Template; Edit Template; Archive Template
	2. CSR User selects option to create new template [A1] [A2]
	3. System displays *Create Template* page including entry fields:
	  a. Language
	  b. Template Category (Dropdown list of categories)
	  c. Template Sub Category (Dropdown list of subcategories)
	  d. Template Name
	  e. Body (Template Text)
	  f. Status (Active, Inactive)
	  g. Tools: HTML editor toolbar

	h. Actions: Submit; Clear; Cancel
	4. CSR User enters form data
	5. CSR User composes template in text field using HTML text editor and selects Submit action
	6. System creates a new template
	7. System displays *List of Templates* page including newly created template
Alternate Paths:	**[A1] CSR User (with sufficient privileges) selects *Edit Template* to modify an existing template:**
	1. System displays *Edit Template* page including:
	a. Language
	b. Template Category
	c. Template Subcategory
	d. Template Name
	e. Body (Template Text)
	f. Status (Active; Inactive)
	g. **Tools**: HTML editor toolbar
	h. **Actions**: Submit; Clear; Cancel
	2. CSR User edits template and selects Submit action [A2]
	3. System updates the template
	4. System displays *List of Templates* page
	[A2] CSR User (with sufficient privileges) selects *Archive Template* to delete a template:
	1. System sets the template status to Inactive
Notes:	There may be 200-300 templates so they are categorized by category and subcategory so that the final selection is from a shorter list.
	Default language is English.
	Templates cannot be deleted, but remain in the system as archived templates.
	If a template exists in both English and Spanish versions, both must be archived separately.
	List can be scrollable list or in pages of 30.
	The system will display different tabs, buttons and links depending on the CSR User's privileges, See the Privileges table below for further details.

Form Validation

NAME	DESCRIPTION	VALIDATION
*Template Name	Title of Template	Alphanumeric. Max Length 60 characters
*Template Body	HTML Text of template	HTML text. Max Length 2048 characters

Privileges

PRIVILEGE	DESCRIPTION	SYSTEM ACTION
Add/Update/Archive Templates	Administrators only have privileges to create, update and archive templates. CSR User with only *Accept, Return and Escalate Case* privilege may only add to or edit existing templates using default fonts.	Show *Templates* tab.

Figure 3.39 – List of Templates

Figure 3.40 – Create a Template
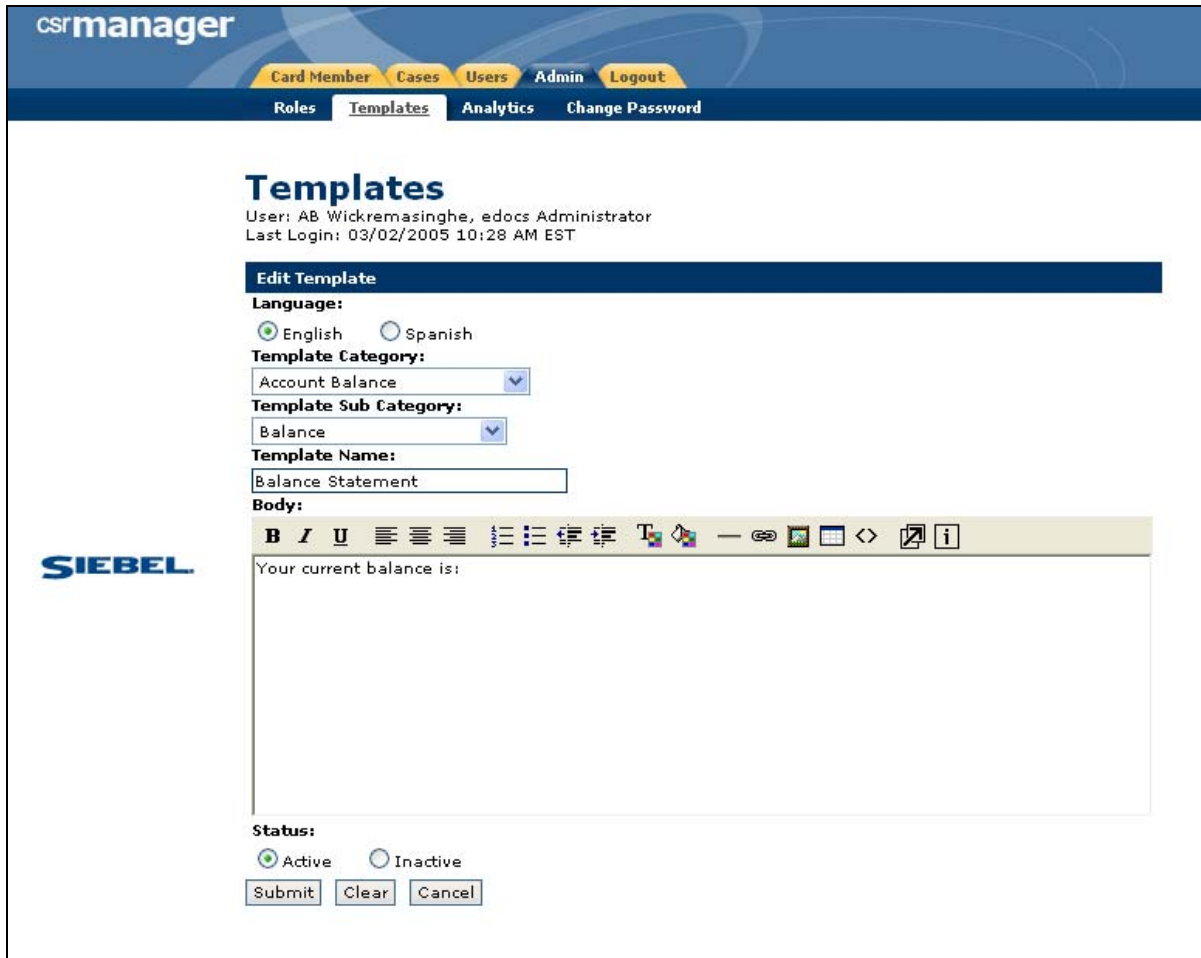
Figure 3.41 – Edit a Template
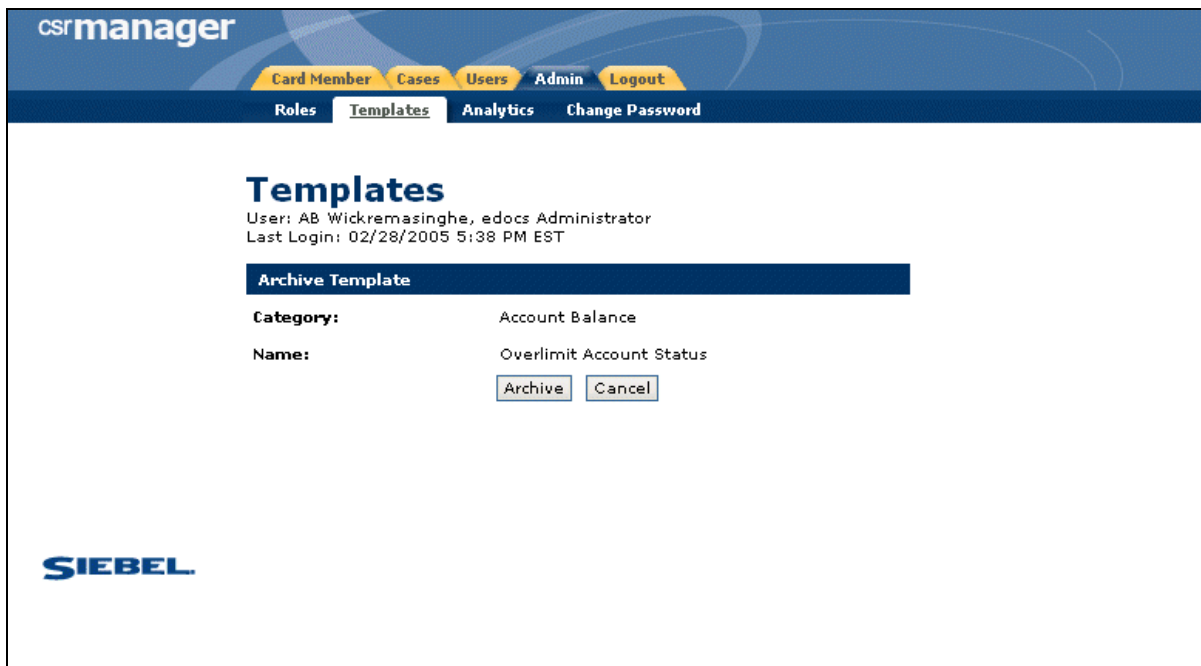
Figure 3.42 – Archive Template Screen

3.4 Analytics

The Analytics use cases cover the business requirements for allowing CSR User's to view informative reports.

1. CSR User Reports – dynamically generate and view a number of reports for monitoring card member and CSR User activity and productivity, including reports on currently locked accounts and User logins:

2. Enrollment and Login Reports – construct and view a report of CSR User case counts by category and user for specified date range

     View Enrollment and User Session Reports

     a) Total Enrolled Card Member Report

     b) Card Member User Session Report

     c) CSR User Session Report

3.4.1 View CSR User Reports (1070)

Name:	View CSR User Reports
Brief Description:	CSR User views reports
Main Path:	1. System displays *List of Reports* page 2. CSR User selects report [A1]-[A9] 3. System displays report

Alternate Path:	**[A1] Case Management Report:**
	 1. System displays options for case report including:
	      a. Report Name (See options below)
	      b. Start Date
	      c. End Date
	      d. Days Open (Min)
	      e. Days Open (Max)
	      f. CSR Users Filter
	      g. Category Filter action
	      h. Status Filter
	      i. **Actions**: Submit; Cancel; Clear
	 2. CSR User selects report parameters
	 3. CSR User selects *Submit* action
	 4. System displays the report summary
	 5. Use case ends
	
	 [A2] Card Member Account Lockout Report:
	 1. System displays a list of all card member accounts that are currently locked out due to registration failures

	a. Card Account (Account Number)
	b. Time Locked (Date and Time Stamp)
	c. Registration Failure Count
	
	[A3] Card Member Lockout Report:
	1. System displays a list of all card members who are currently locked out due to login failures
	   a. Account Number
	   b. User ID
	   c. Time Locked (Date and Time Stamp)
	   d. Login Failure Count
	
	[A4] CSR User Lockout Report:
	1. System displays a list of all CSR Users who are currently locked out due to login failures
	   a. Login ID
	   b. User Name
	   c. Time Locked (Date and Time Stamp)
	   d. Lockout Reason
	   e. Login Failure Count
	
	[A5] Total Enrolled Card Members Report:
	1. System displays a list of enrolled card members:
	   ▪ Number of Enrolled Card Members
	
	[A6] Card Member Session Report:
	1. System displays a list of all open card member sessions
	   a. Account Number
	   b. User Name
	   c. User ID
	   d. Logged On (Date and Time Stamp of Login)
	
	[A7] CSR User Session Report:
	1. System displays a list of all open CSR User Sessions
	   a. CSR Login ID
	   b. CSR User Name
	   c. Date and Time Stamp of Login

Business Rules:	**[B1]** CSR Users will only be allowed to see reports for categories that they have been assigned to.

Notes:	Pages that have sensitive information that would enable take over include: Profile; Payment summary; QuickPay; Scheduled; Statement; Statement History. These would be ones that would need to be tracked if CSR User logs on as user. To simplify: track every page.
	
	The system will display different tabs, buttons and links depending on the CSR User's privileges, See the table below for further details.
	
	The options for the Case Management Report are:
	   ▪ *Analyze CSR Case Load* – provides key information concerning the current work load of one or more CSR Users. This report is used in conjunction with the *Reassign Case* feature.
	   ▪ *Analyze Case Load by Type* – provides key information as to the

types of cases that are currently being worked on or that have been worked on over a period of time. This information can be used to ensure that categories are properly staffed.

- *Cases Closed* – provides key information as to the rate of cases closed over time for one or more CSR User. This information can be used to evaluate the effectiveness of one or more CSR User.

- *Cases Overdue* – provides cases that have been open longer than the specified maximum (48 hours). This report can be used in conjunction with the *Reassign Cases* option so that overdue cases can be quickly reassigned to another CSR User who may have a lesser case load.

- *Escalated Cases by User* – provides all cases by user which have been escalated. This report can be used to determine which CSR Users are escalating cases instead of closing them.

The report names for the Case Management Reports are:

1. Group by Categories, Case Count report columns:
   a. Categories (Drilldown)
   b. Count
   c. Percent

- Group by CSR, Case Count report columns:
   a. CSR Name (Drilldown)
   b. Count
   c. Percent

2. Group by Case Days Open, Case Count report columns:
   a. Case Days Open (Drilldown)
   b. Count
   c. Percent

3. Group by Case Status, Case Count report columns:
   a. Case Status (Drilldown)
   b. Count
   c. Percent

4. CSR Cases Closed report columns:
   a. CSR Name (Drilldown)
   b. Count
   c. Percent

5. Escalated Cases by CSR report columns:
   a. CSR Name (Drilldown)
   b. Count
   c. Percent

6. Escalated Cases by Category report columns:
   a. Categories (Drilldown)
   b. Count
   c. Percent

7. Activity by Event Type report columns:
   a. Event Type (Drilldown)
   b. Count
   c. Percent

	All Drilldown: report columns:
	a. Case No.
	b. Created
	c. Last Updated
	d. Card Member Name
	e. Category
	f. Status
	g. Owner

Privileges

PRIVILEGE	DESCRIPTION	SYSTEM ACTION
View Reports	Fraud Reps and managers are allowed to view reports of CSR User activity.	Show *Analytics* sub-tab. Show all Reports
View Card Member Profile	CSR Users with this privilege may see Card Member Session report.	Show *Analytics* sub-tab. Show Card Member Session Report
Assign Case	CSR Users with this privilege may see Case Management Reports for users in their categories.	Show *Analytics* sub-tab. Show Case Management Report
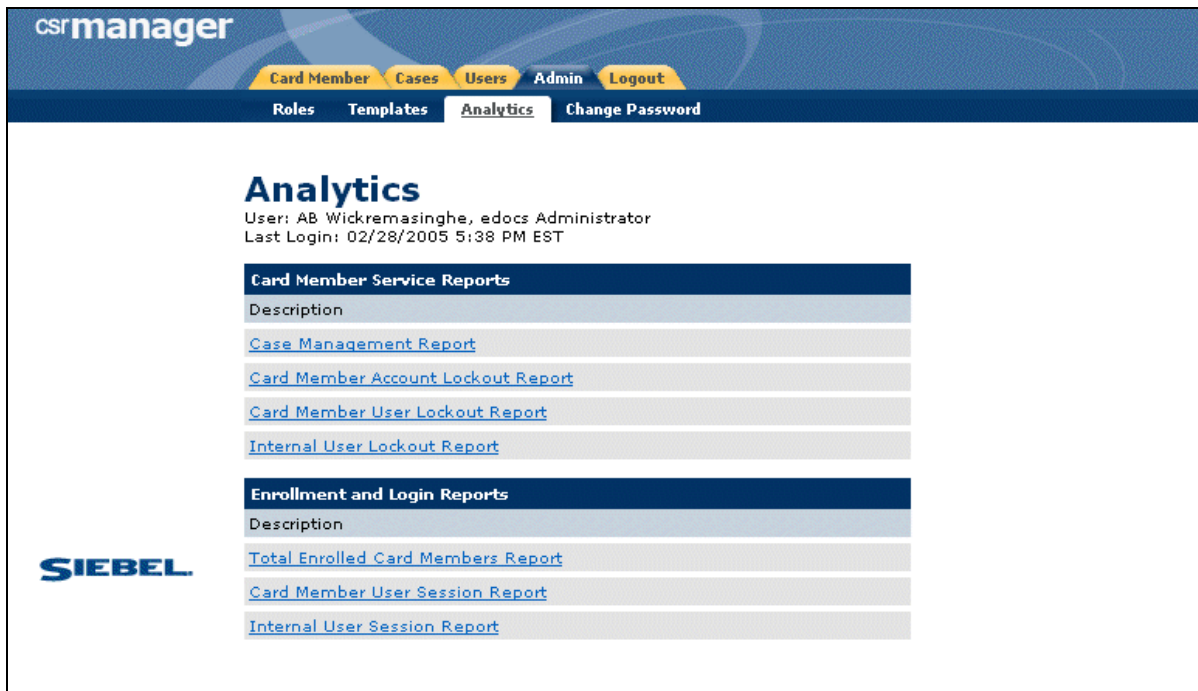
Figure 3.43 – Analytics Dashboard of Reports

Figure 3.44 – Case Management Report Criteria
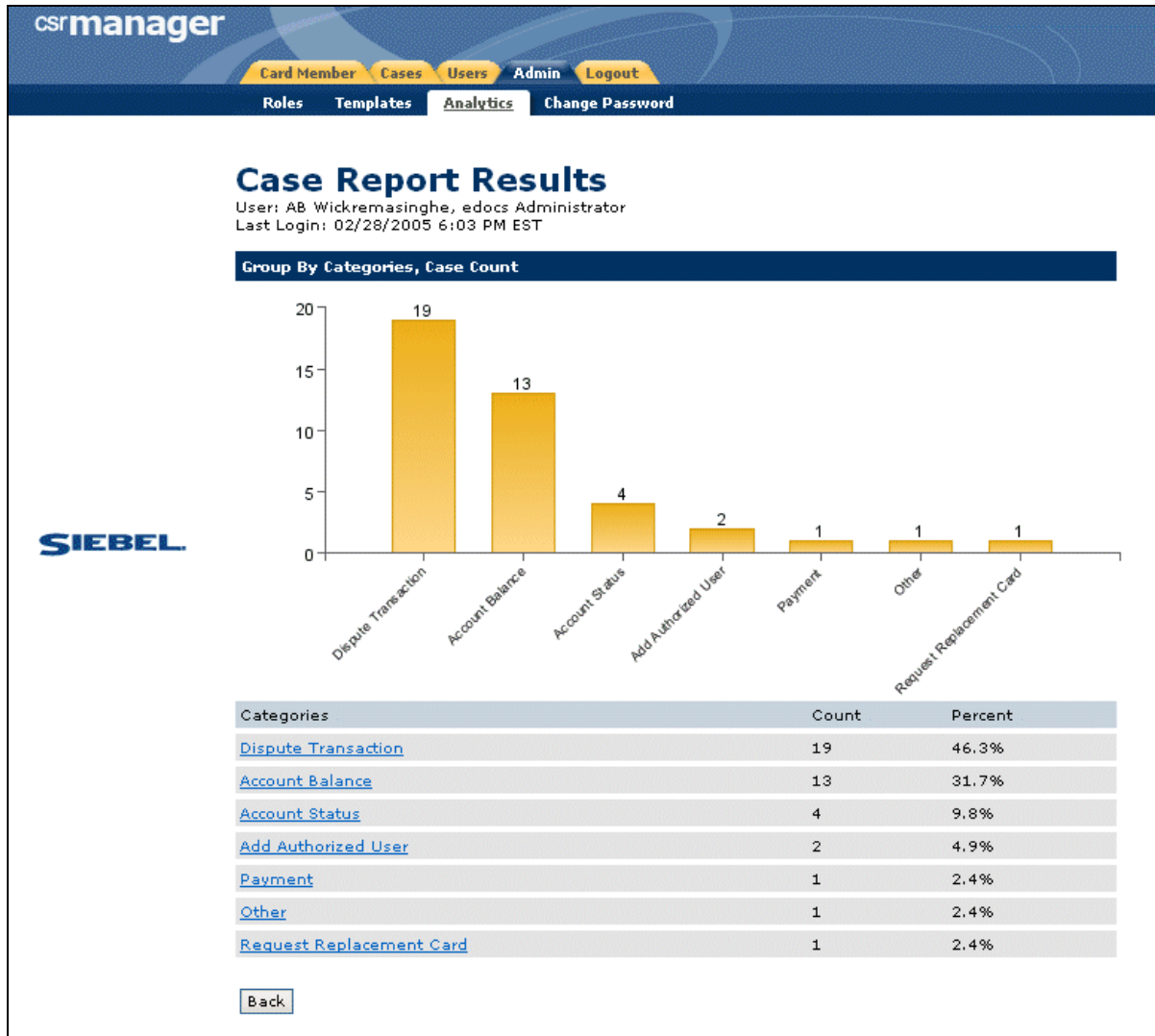
Figure 3.45 – Case Management Report Results: Group by Categories, Case Count

Case Report Results

User: AB Wickremasinghe, edocs Administrator
Last Login: 02/28/2005 6:03 PM EST

Group By Categories, Case Count : Account Balance

Page 1 of 1

Case No.	Created	Last Updated	Card Member Name	Category	Category	Owner
1000041	02/01/2005 11:34PM	02/01/2005 11:34PM	Garner Mary Loug	Account Balance	Closed	CSR Case Queue
1000022	12/09/2004 07:54PM	01/13/2005 10:10PM	Short Debbie	Account Balance	Open	Abbott, Joel
1000005	11/15/2004 04:21PM	11/15/2004 04:24PM	James Greg	Account Balance	Closed	Yedla, Usha
1000017	11/30/2004 07:37PM	12/08/2004 10:53PM	James Greg	Account Balance	Open	Albert, Lev
1000020	12/06/2004 10:38PM	12/08/2004 10:53PM	Short Debbie	Account Balance	Open	Albert, Lev
1000021	12/09/2004 05:23PM	12/09/2004 07:40PM	Short Debbie	Account Balance	Closed	Yedla, Usha
1000003	11/15/2004 12:08PM	11/15/2004 05:29PM	Garner MaryLou	Account Balance	Closed	Yedla, Usha
101001	10/27/2004 04:14PM	10/27/2004 04:28PM	Gault, John (10)	Account Balance	Closed	Albert, Lev
101002	10/27/2004 04:30PM	10/27/2004 04:41PM	Gault, John (10)	Account Balance	Closed	Albert, Lev
101003	10/27/2004 04:45PM	11/30/2004 07:46PM	Gault, John (10)	Account Balance	Closed	Wickremasinghe, AB
102021	11/09/2004 09:02AM	11/30/2004 07:46PM	Gault, John (10)	Account Balance	Closed	Albert, Lev
1000001	11/11/2004 01:35PM	12/08/2004 10:52PM	Garner MaryLou	Account Balance	Open	Albert, Lev
1000048	02/18/2005 02:04AM	02/28/2005 03:54PM	Garner Mary Loug	Account Balance	Open	CSR Case Queue

Back

Figure 3.46 – Case Management Report Drill-Down: Group by Categories, Case Count
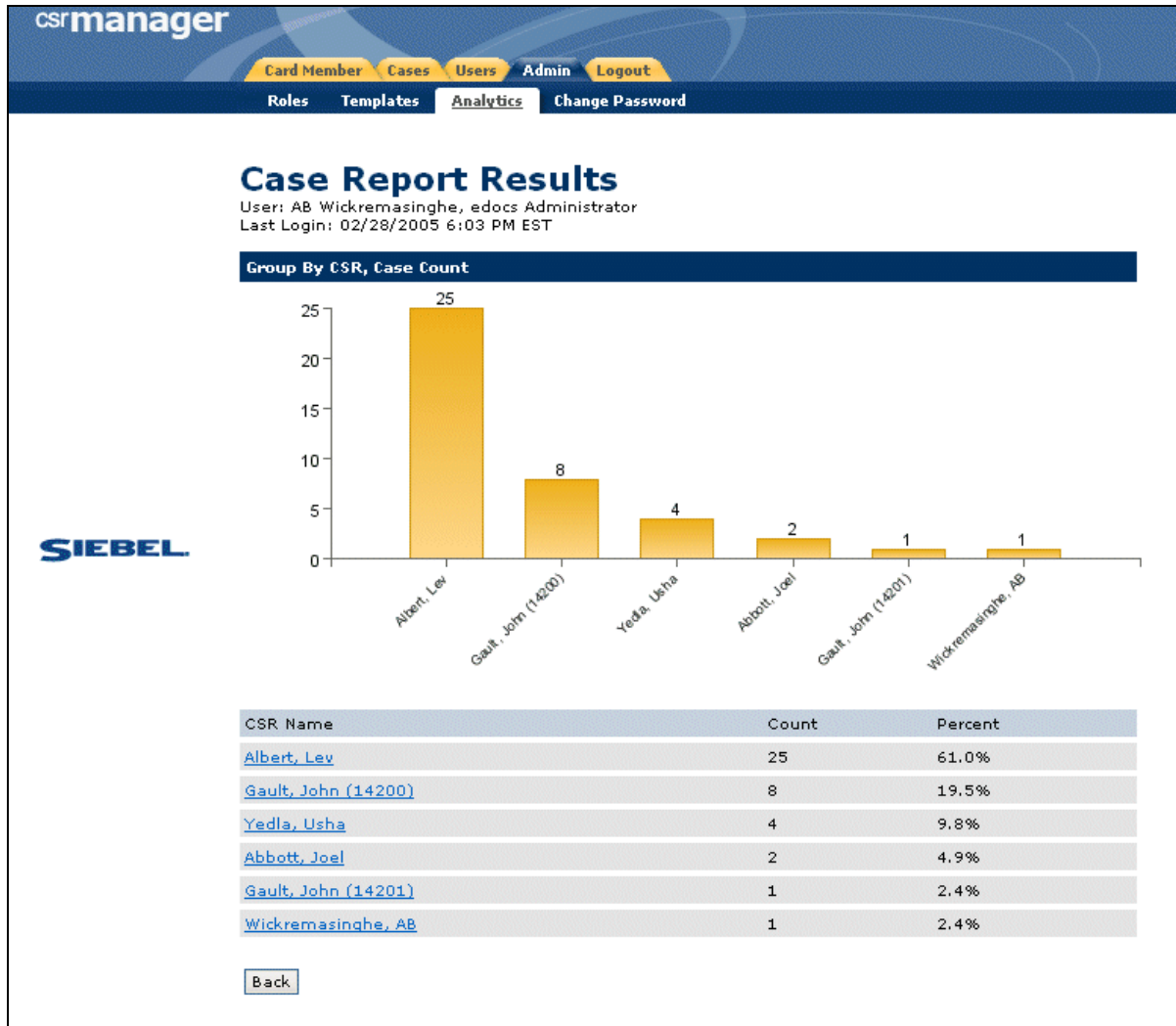
Figure 3.47 – Case Management Report Results: Group by CSR, Case Count

Figure 3.48 – Case Management Report Drill-Down: Group by CSR, Case Count
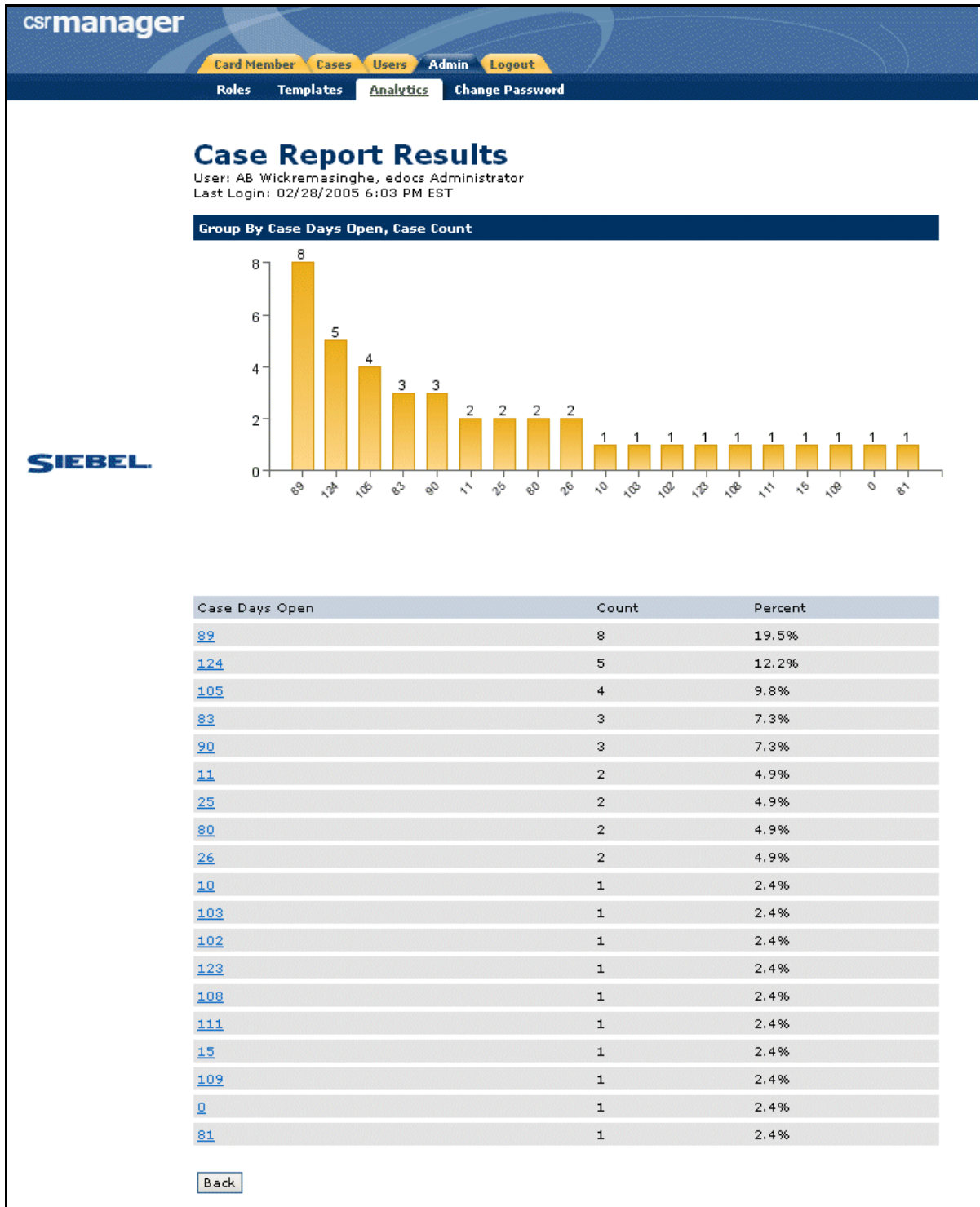
Figure 3.49 – Case Management Report Results: Group by Case Days Open, Case Count

Figure 3.40 – Case Management Report Drill-Down: Group by Case Days Open, Case Count

Figure 3.41 – Case Management Report Results: Group by Case Status, Case Count

Figure 3.42 – Case Management Report Drill-Down: Group by Case Status, Case Count
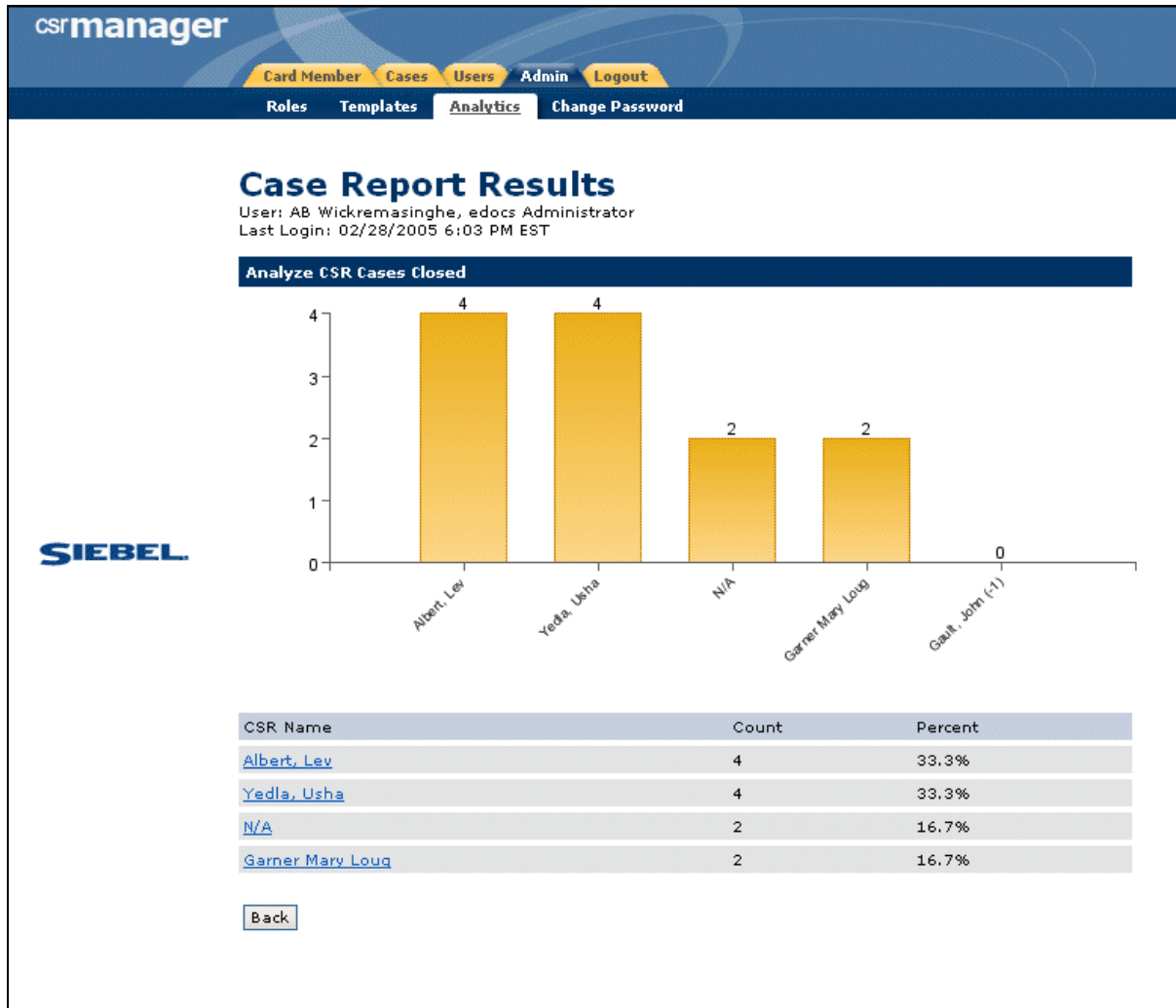
Figure 3.43 – Case Management Report Results: CSR Cases Closed

Figure 3.44 – Case Management Report Drill-Down: CSR Cases Closed
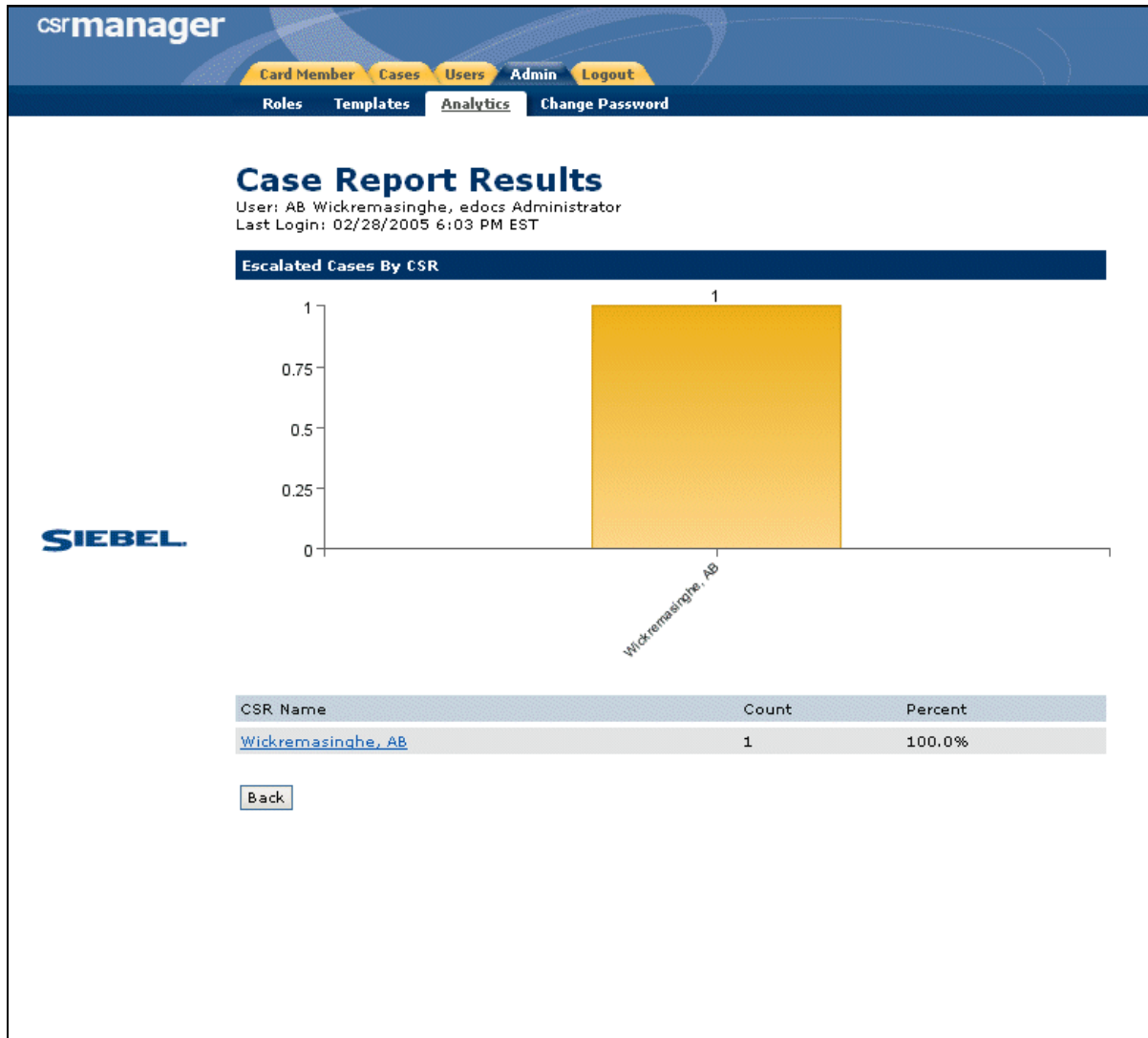
Figure 3.45 – Case Management Report Results: Escalated Cases by CSR

Figure 3.46 – Case Management Report Drill-Down: Escalated Cases by CSR

Figure 3.47 – Case Management Report Results: Escalated Cases by Category

Figure 3.48 – Case Management Report Drill-Down: Escalated Cases by Category

Figure 3.49 – Case Management Report Results: Activity by Event Type

Figure 3.50 – Case Management Report Drill-Down: Activity by Event Type

Figure 3.51 – Card Member Account Lockout Report

Figure 3.52 – Card Member User Lockout Report
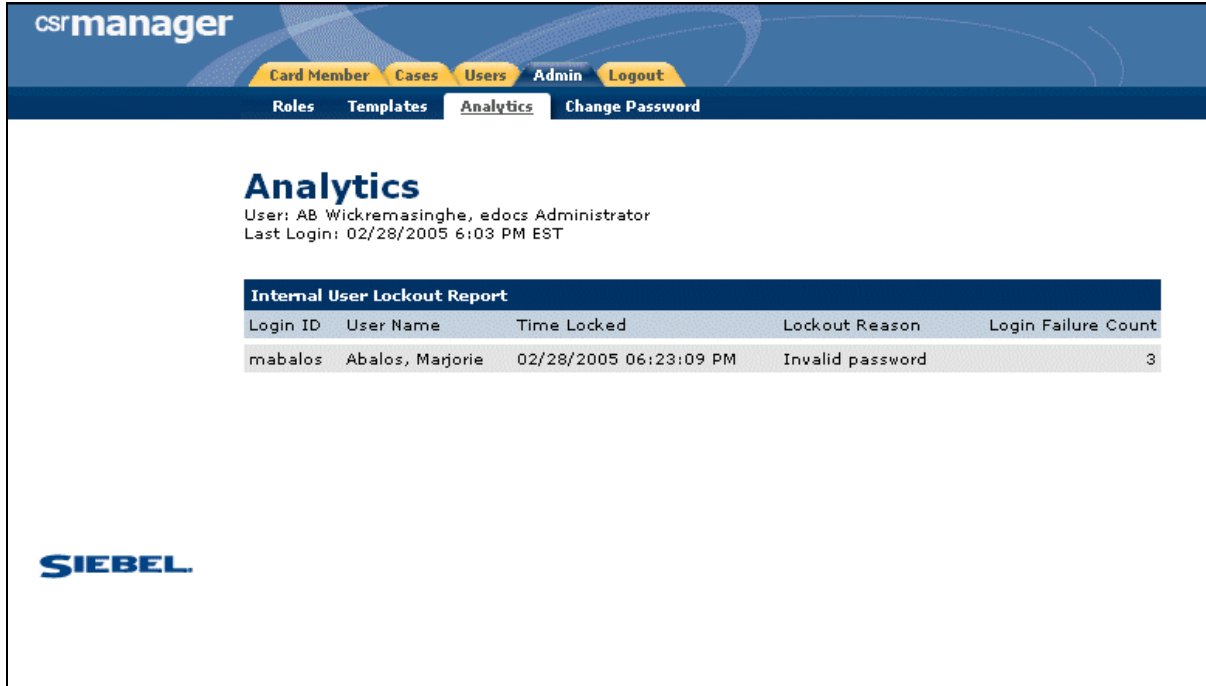
Figure 3.53 – Internal User Lockout Report
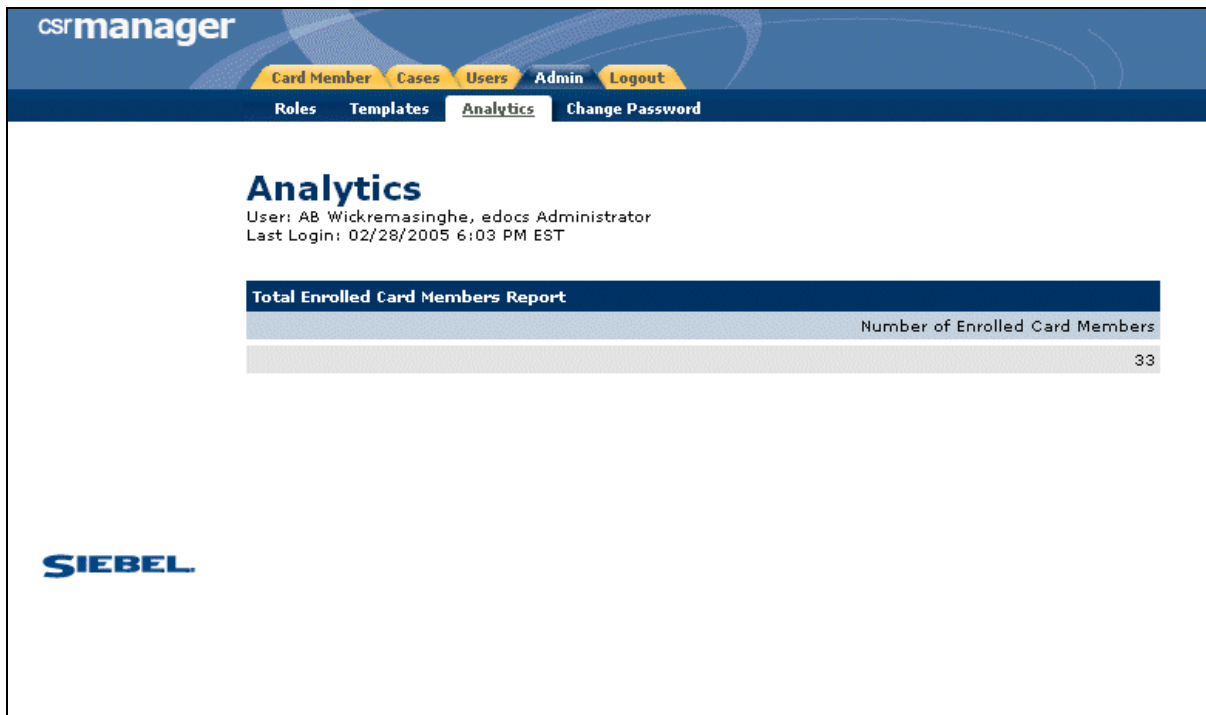
Figure 3.54 – Total Enrolled Card Members Report

Figure 3.55 – Card Member User Session Report

Figure 3.56 – Internal User Session Report

4.1 Daily Activity Reports

This section describes the use cases for the following reports:

- **Card Member Activity Report**
- **Card Member Profile Change Report**
- **Payment Report**
- **Direct Bill Pay Report**
- **Address Change Report**
- **Card Member Lockout Report**
- **Internal User Lockout Report**
- **Secure Messaging Report**

4.1.1 Card Member Activity Report (1200)

Name:	Card Member Activity Report
Report Description:	Card Member Activity Report tracks online card member activity including enrollment events, login event, log out or timeout events, view statement, and send a secure message.
Delivery Format	CSV
Delivery Method	FTP
Delivery Location	TBD
Report Contents:	Report contains the following fields: 1. Card Member Account Number 2. Date and Time Stamp 3. Activity Code 4. Language Indicator 5. IP Address

Notes:	The Activity Report runs Midnight – Midnight. The list of Activity Codes and corresponding Activity Data is provided in the attached file. Final CM_Activity Codes.xls (1… The purpose of this report is to track the activities that card members perform and not to report on the data entered by card members, so this report does not contain any activity data. Other reports such as the Payment Report will capture transaction data.

4.1.2 Card Member Profile Change Report (1205)

Name:	Card Member Profile Change Report
Report Description:	Card Member User Profile Change Report lists Card Member user profile changes, which include all Address fields, Home Phone Number, Business Phone Number, Email Address, Password and Language Indicator
Delivery Format	CSV
Delivery Method	FTP
Delivery Location	TBD
Report Contents:	Report Contains: 1. Card Member Account Number 2. Date and Time Stamp 3. Profile Change Type 4. Card Member's Old Value 5. Card Member's New Value 6. Profile Change Count 7. Home Phone Change Count 8. Business Phone Change Count
Notes	The Activity Report runs Midnight – Midnight.

4.1.3 Payment Report (1210)

Name:	**Payment Report**
Report Description:	Payment Report tracks all card member daily online payments.
Delivery Format	CSV

Delivery Method	FTP
Report Contents:	Report Contains: **1.** Card Member Account Number **2.** Checking Card Member Account Number **3.** Account Type (Checking, Savings) **4.** Payment Type (Scheduled, One-Time, Recurring) **5.** Transit/Routing # **6.** Payment Amount **7.** Date and Time Stamp **8.** Transaction ID
Notes:	Runs from 7pm EST – 6:59 pm EST. The reports should be created seven times a week

4.1.4 Pay Other Bill Report (1220)

Name:	**Pay Other Bills Report (Corresponds to Pay Other Bills use case)**
Report Description:	Pay Other Bills Report tracks all card member activity for the Pay Other Bills Program.
Delivery Format	CSV
Delivery Method	FTP
Delivery Location	TBD
Report Contents:	Report Contains: **1.** Card Member Account Number **2.** Date and Time Stamp **3.** Payee Name **4.** Payee Address **5.** Payee City **6.** Payee State **7.** Payee ZIP **8.** Payee Card Member Account Number **9.** Payee Payment Amount **10.** Ticket Terms Code **11.** Direct Bill Pay Flag (Value=Z) **12.** Available Credit at time of transaction
Notes:	

4.1.5 Address Change Report (1230)

Name:	**Address Change Report**
Report Description:	The Address Change Report provides a list of all accounts where potential fraud may be occurring. The change types tracked are same day as enrollment, same day as forgot password, and same new address as another address change today or during previous day
Delivery Format	CSV
Delivery Method	FTP
Report Contents	Report Contains: **1.** Card Member Account Number **2.** Date and Time Stamp **3.** Change Type **4.** Card Member's Old Address **5.** Card Member's New Address
Notes	This report: Provides a list of all accounts where an address change was requested on the same day as enrollment, re-enrollment or forgot password. Provides a list of all accounts that have changed their address to a new address that is IDENTICAL to a new address on a previous address change that occurred the same day or during the previous calendar day.

4.1.6 Card Member Lockout Report (1240)

Name:	**Card Member Lockout Report**
Report Description:	The Card Member Lockout Report lists card members that have become locked out due to login and registration failures.
Delivery Format	CSV
Delivery Method	FTP
Report Contents:	Report Contains: **1.** Card Member Account Number **2.** Date and Time Stamp **3.** Card Member User Login Failure Count **4.** Account Registration Failure Count

4.1.7 Internal User Lockout Report (1242)

Name:	**Internal User Lockout Report**
Report Description:	The Internal User Lockout Report lists CSR Users that become locked out due to login failures and password expiration.
Delivery Format	CSV
Delivery Method	FTP
Report Contents:	Report Contains: **1.** Internal Login ID **2.** Internal User Name **3.** Date and Time Stamp **4.** Lockout Reason (Invalid Password, Inactive, Expired) **5.** Internal User Login Failure Count

4.1.8 Secure Messaging Report (1330)

Name:	**Secure Messaging Report**
Brief Description:	The Secure Messaging Report shows case management productivity for all CSR Users
Delivery Format	CSV
Delivery Method	FTP
Delivery Location	TBD
Main Path:	Report Contains: **1.** New/Processed Item (0=not worked; 1=worked) **2.** Case ID Number **3.** Inquiry Date/Time (Date Created) **4.** Card Member Account Number **5.** Processed Date/Time (Date Updated, if processed by rep) **6.** Internal Login ID (if processed by a rep, i.e., New/Processed Item = 1) **7.** Language Indicator (en_US=English; es_US =Spanish) **8.** Template Name (if processed by rep)
Notes:	Category code is length 2. Category code relates to CSR User categories

4.2 Daily Security Reports

This section describes the use cases for the following reports:

- **Internal Users Activity Report**
- **Internal User Role Report**
- **Internal User Profile Change Report**
- **Internal User Security Violation Report**

4.2.1 Internal Users Activity Report (1300)

Name:	Internal Users Activity Report
Report Description:	Internal Users Activity Report serves to detect fraudulent activity of the CSR Users who have access to card member data. The report is twofold: it tracks CSR User activity in the CSR User application and it tracks action made on behalf of card member (tracking the same information as the Card Member Activity Report). CSR User activity includes searching card member by SSN, jumping to page, resetting password, unlocking card member, unlocking account number, unlocking CSR User, changing CSR User Status (active or inactive) and changing card member user status (active or inactive).
Delivery Format	CSV
Delivery Location	TBD
Report Contents:	Report Contains: 1. Internal Login ID 2. Date and Time Stamp 3. Internal User Activity Name (Code) 4. Activity Data
Notes:	Jump to Page jumps to the first page of a series of pages and will not necessarily show the page the CM is currently on. It will also not show data that the CM has entered into a form.

4.2.2 Internal User Role Report (1310)

Name:	Internal User Role Report
Report Description:	The Internal User Role Report lists all CSR Users and their roles and privileges. *CSR User statuses tracked are active or inactive only.*
Delivery Format	CSV
Delivery Location	TBD

Report Contents:	Report Contains:
	1. CSR User Name
	2. Internal Login ID
	3. Status
	4. Role
	5. Privileges
	6. Categories (Case Management)
	7. Escalation or No Escalation (Case Management)
	8. Date and Time Stamp of Last Login

4.2.3 Internal User Profile Change Report (1320)

Name:	**Internal User Profile Change Report**
Report Description:	The Internal User Profile Change lists all changes to the CSR User's profile. A c*hange is defined as addition, deletion, and update, where applicable, to Case Management categories, roles, privileges, escalation, status (active or inactive), password, and language indicator.*
Delivery Format	CSV
Delivery Method	FTP
Report Contents:	Report Contains:
	1. Internal User Name of person making change
	2. Internal Login ID of person making change
	3. Date and Time Stamp of change
	4. Changed Internal User Name
	5. Changed Internal Login ID
	6. Change Type
	7. Change Data
	8. Internal User Change Count

4.2.4 Internal User Security Violation Report (1330)

Name:	**Internal User Security Violation Report**
Report Description:	This report tracks failed login attempts by internal admin users and the reason for the failure.
Delivery Format	CSV
Delivery Method	FTP

Report Contents:	Report Contains: **1.** Internal User Name **2.** Internal Login ID **3.** Date and Time Stamp **4.** Reason Failed **5.** IP Source

4.3 Daily System Reports

This section describes the use cases for the following reports:

- **User Information Report**

- **E-Mail Notification Report**

- **File Reconciliation Report**

4.3.1 User Information Report (1410)

Name:	**User Information Report**
Report Description:	The User Information Report shows enrollment and log in report. This report will report on enrollments, logins and statement views for the given day (from midnight to midnight)
Delivery Format	CSV
Delivery Location	TBD
Report Contents:	Report Contains: **1.** Date and Time Stamp **2.** Number of Logins **3.** Number of Distinct Users **4.** Number of New Enrolled Users **5.** Number of Statements Viewed

4.3.2 E-mail Notification Report (1420)

Name:	**E-mail Failure Report**
Report Description:	The E-mail Notification Report lists e-mails that have been sent by Siebel Self-Service for Cards
Delivery Format	CSV
Delivery Method	FTP

Report Contents:	Report Contains:
	1. Date and Time Stamp
	2. Time Stamp for Email Job Start
	3. Time Stamp for Email Job Finish
	4. Card Member Account Number
	5. Card Member E-mail Address
	6. E-mail Title

4.3.3 File Reconciliation Report (1430)

Name:	**File Reconciliation Report**
Report Description:	The File Reconciliation Report tracks the number of statements (primary keys) processed.
Delivery Format	CSV
Delivery Method	e-mail
Report Contents:	Report Contains:
	1. Date and Time Stamp
	2. File Type
	3. File Name
	4. File Size (MB)
	5. File Load Time
	6. Statement Count
	7. Record Count
Notes:	The report can be in the body of the e-mail
	The e-mail tile should be descriptive: include File Type; Date

5   User Interface

5.1 Introduction

This section outlines the User Interface (UI) of the system. The solution will be compatible for the following browsers:

- IE 5.X and above

- Netscape 7.X and above

- Firefox 0.9

5.2 Accessibility

The Siebel Self-Service for Cards website will be handicap accessible. The details of the accessibility are TBD and will be delivered in a separate document.

5.3 Browser Window Title

The title presented in the browser window will be "Siebel Self-Service for Cards brought to you by Siebel Systems"

6

External Interfaces

6.1 Overview

Siebel Self-Service for Cards supports the FDR billing system's statement data file, Monetary, and Delta (Change Data) file formats. Other interfaces for other billing systems such as TSYS may be supported upon customer request.

♦ **Billing System Statement Files** – contain statement data generated and delivered by the billing system to the Siebel Self-Service for Cards Platform for each monthly billing cycle

♦ **Billing System Monetary Files** – contain daily payment transactions generated and delivered by the billing system to the Siebel Self-Service for Cards Platform

♦ **Billing System Change Data (CHD) File** – the billing system to the Siebel Self-Service for Cards Platform

♦ **ACH Payment File** – contains online payments processed by the payment module and delivered by the Siebel Self-Service for Cards Platform to the billing system

Batch Processing consist of following steps:

♦ File delivery by the billing system

♦ Pre-processing

♦ Upload processing

♦ File generation by Siebel Self-Service for Cards Platform

♦ File delivery by Siebel Self-Service for Cards Platform

The batch processing tasks have recoverability in the event of any kind of failure like network, system or database. Database Back-up will be performed after uploading the data from the billing system delivered files and then only billing system delivered files will be removed from the system.

Note: Response header may not be needed

ID	NAME	DESCRIPTION	LENGTH
1	Filler		32
2	Batch Type Code	Value = 9 (Non-Monetary Batch Header	1

		Record)	
3	Filler	Must be spaces	2
4	Batch Number	Numeric	5
5	Drop Debit Ticket File Indicator	Value = D	1
6	Ticket File Batch Date	Format = MMDD	4
7	Filler	Must be spaces	2
8	System Number	Numeric = 5994	4
9	Filler	Must be spaces	2
10	Principal User Number	Principal Bank Number for Cardholder Numeric	4
11	Filler	Must be spaces	22
12	Terminal ID	Numeric	4
13	Operator Code	Numeric	2

Figure 6.1 – Payment File Batch Header

ID	NAME	DESCRIPTION	LENGTH
1	Cardholder Account Number	Alphanumeric with check digit and trailing spaces	16
2	Transaction Code	Numeric with leading zeros	3
3	Account Number	Add or change banking information 021 = Checking Account (Alphanumeric, Variable Length Field Max Length = 17) 024 = Savings Account (Alphanumeric, Variable Length Field Max Length = 10) 053 = Transit Routing Number (Numeric Length = 9)	17 (Checking) 17 (Savings) 9 (Routing Number)
4	Filler	Must be spaces	38 (Checking) 38 (Savings) 46 (Routing)
5	Terminal ID	Numeric	4
6	Operator Code	Numeric	2

Figure 6.2 – Account Information Transaction

ID	NAME	DESCRIPTION	LENGTH
1	Cardholder Account Number	Alphanumeric with check digit and trailing spaces	16
2	Transaction Code	Numeric with leading zeros	3
3	T759-SUB-TRAN	Numeric	2
5	Payment Amount	T759-ACH-PMNT-AMT Numeric with two decimal places 9(15)V99	17
6	Payment Type	Values = C (Checking), S (Savings)	1
7	Filler	Spaces	35
8	Terminal ID	Numeric	4
9	Operator Code	Numeric	2

Figure 6.3 – Payment Transaction

ID	NAME	DESCRIPTION	LENGTH
1	Blank Test Area	Must be spaces	31
2	Header Type	Value = 01	2
3	Client Number	Value = D	4
4	User ID Text	Alphanumeric (Upper Case)	6
5	Record Input Counter	Numeric	8
6	Sequence Number	Alphanumeric	5
7	Filler	Alphanumeric	24

Figure 6.4 – Response Header Format

6.1.1 ACH Returns

No ACH return file processing is required.

6.1.2 Format Updates

Billing system issues updates to file formats six times a year. These may result in the requirement to change Siebel Self-Service for Cards pre-processors. Such changes are out of the scope of the work defined by this document and would be handled under a separate Statement Of Work.

6.1.3 Cycle (MSR) File

	VALUE	NOTES
Size	2 GB	Estimate based on past records
Delivery Time	3:00AM-7:00 AM	Kicked off after midnight Download time 270 mins (DS3) Window for scheduling job: (5am – 11am)
Delivery Location	See Billing System	
Frequency	Sun-Fri	6 times a week (not Saturday) Except if Saturday is last day of month, in which case it will be on Saturday instead of Sunday.
Record Layout		See MSR File Mapping Document

6.1.4 Monetary File (MON)

The Daily Monetary file contains the all the daily transactions posted to an account for the previous day. This includes, online payments, non-online payments, credits and returns and purchases. (It does not contain non-billed authorizations).

	VALUE	NOTES
Size	.5 GB	Estimated based on past records
Delivery Time	1:00 AM	Kicked off after midnight CST
Delivery Location	See Billing System	
Frequency	Sun-Fri	6 times a week (not Saturday) Except if Saturday is last day of month, in which case it will be on Saturday instead of Sunday.
Record Layout		See Monetary File Format Document

6.1.5 Change Data (CHD) File

Change Data file is a file that gets generated everyday. It only contains accounts when something has changed on an account. For example: Current Balance changed due to payment made by card member or a card was reported lost or stolen. The file is generated even if it contains no records. (See CHD File Format Document)

	VALUE	NOTES
Size	1-4 GB	IGB per day sometime up to 4GB
Delivery Time	270 mins (DS3)	Kicked off after midnight Download time Window for scheduling job (4am – 6am)
Delivery Location	See Billing System	
Frequency	Sun-Fri	6 times a week (not Saturday) Except if Saturday is last day of month, in which case it will be on Saturday instead of Sunday.
Record Layout		See CHD File Format Document

6.2 FDR Real-Time Interfaces

6.2.1 Overview
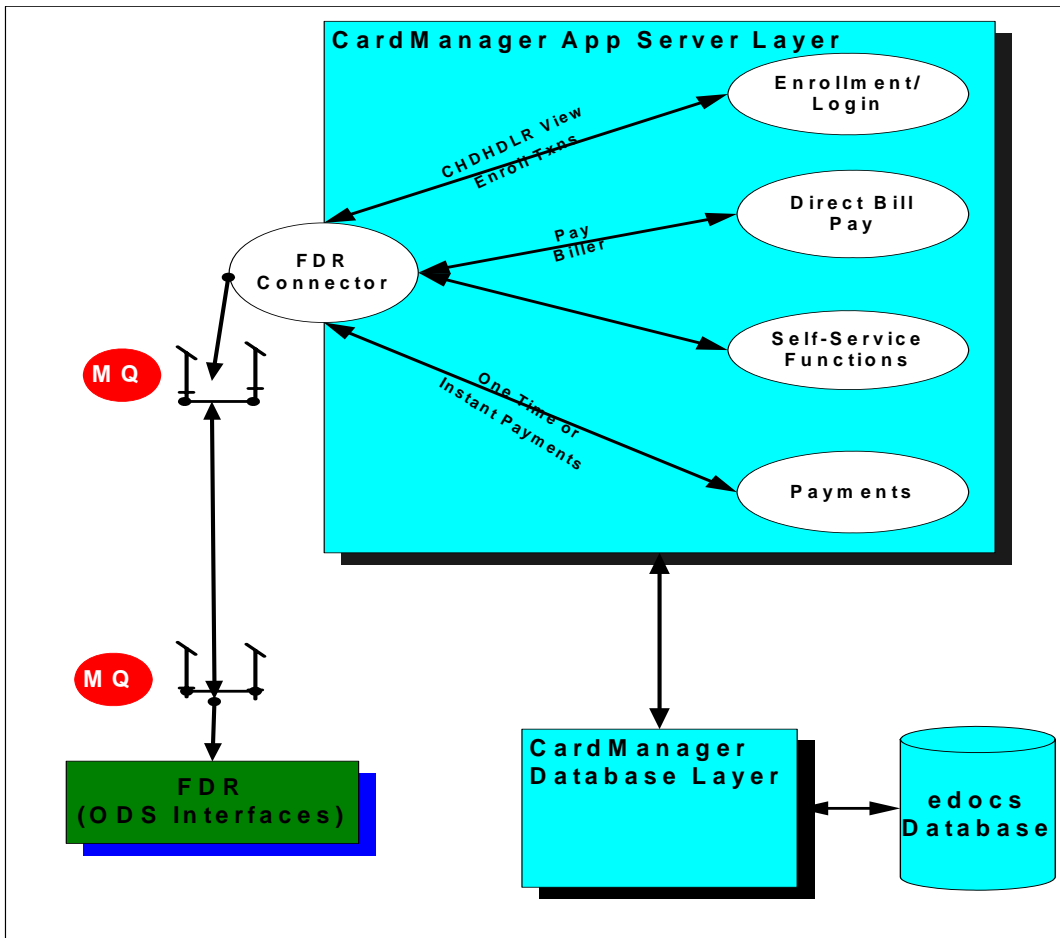
Figure 6.5 – Siebel Self-Service for Cards Real-Time Interfaces

FDR real-time interface consists of a set of ODS calls. These are messages to an FDR MQSeries server in Omaha. Since there is a cost for each transaction, the number of calls will be minimized as far as possible within performance constraints.

6.2.2 ODS Calls By Feature

The following table summarizes ODS calls made to support Siebel Self-Service for Cards features. See also a spreadsheet with full details of the ODS calls.

FEATURE	CALLS	ACTIONS
Enroll	CHDHLDR EMBOSS_TEMP INTERNET_ADDRESS_INFORMATION CNONMON CARD_ISSUANCE_PLASTIC	Get profile information for validation Get CVV information for validation using expiration date. Get External and Internal statuses to determine whether card member is allowed to enroll. Send updated e-mail address Set Enrolled Flag (Misc_8_5 field)
Update Profile	CHDHLDR CAP CHDMEMO CNONMON	Check status codes to determine whether card member can view Personal Details. Send update to change info on FDR. Send memo for profile change: phone
Login/Account Summary	CHDHLDR CARDHOLDER_SPECIAL CREDIT_LIFE_INSURANCE	Get profile information for display Determine what important messages should be displayed. Get External and Internal statuses to determine whether card member is allowed to log in and what features card member is allowed to see and use. Check insurance flag, portfolio flag and status codes to determine whether card member is eligible for Account Protection Plus (APP). Check status codes and Number of Plastics to determine whether eligible for Direct Bill Pay. (In which case Direct Bill Pay tab will be displayed)
Manage Alerts	CHDHLDR	Get current values of balance
Make Direct Bill Payment	BALANCE_CONSOLIDATION	Send request to make a balance transfer using locally stored Payee information.
Make/View Payment	CHDHLDR CNONMON	Get current card member profile information for display Send payment request
Manage Bank Accounts	CNONMON	Send bank information on first enroll Get bank information for checking repaired bank information (EPICWare issue).

Order Service	CHDHLDR CAP	Check statuses to determine what services are available. Check days delinquent not > 40
Convenience Checks (SS)	CNONMON	Last Check Number parameter = 2000
Suppress Paper (SS)	CNONMON CHDHLDR	Held Destination Code set to "W" Statement Hold Code (CHDHLDR) Misc Field 10, Pos 6 (E=Eligible)
Request Replacement Card (SS)	CHDHLDR CARD_ISSUANCE_PRODUCT CAP	Need to display primary and secondary user and check for auth users Sequence number must be 0001 (Primary) or 0002 (Secondary) Need to check if the card is in the reissue process
Add Authorized User (SS)	CAP	Name must not match existing auth user Sequence number 0003-0250 for additional authorized users. Need to check if the card is in the reissue process
Dispute (SS)	CHDHLDR	Get current card member account number and Address, home and work phone number
Handle Card Member Inquiry	CHDHLDR INTERNET_ADDRESS_INFORMATION CARD_ISSUANCE	Get following card member profile and status information so that card member profile can display: Primary Name;Paper Off Eligible Flag; Paper Hold Flag;Direct Bill Pay Eligible Flag; Balance Transfer Eligible Flag; External and Internal Status Codes; Social Security Name; Billing Zip Code; Product Code (Brand); E-mail Address; Convenience Check Eligible; Replacement Card Eligible; Add Auth Eligible

Figure 6.6 – Features That Use ODS Calls

6.2.3 ODS Business Rules By Field

The following table provides a cross-reference for ODS fields used in business rules.

FIELD	VALUES	BUSINESS RULE	USE CASE
External Status	A, B, L, U, Z, F, I, or C (with balance is zero or negative)	B2 Enroll Display	1000 Enroll
External Status	A, B, L, U, Z, F, I, or C (with balance is zero or	B1 Login Display	1110 Login

	negative)		
Internal Status	X	B1 Acct Summary Intuitive Messages	1340 View Account Summary
Internal Status	D	B1 Acct Summary Intuitive Messages	1340 View Account Summary
Internal Status	O	B1 Acct Summary Intuitive Messages	1340 View Account Summary
External Status	C	B1 Services Display	1890 Order Service
External Status & Internal Status	External Status is E OR ((Internal Status of D OR X AND Days Delinquent > 40):	B2 Services Display	1890 Order Service
Product Type Code	= Secured Product Type (See Product Type code mapping table.	B2 Services Display	1890 Order Service
Auth Users, Primary Name, Secondary Name	TBD	B1 Add Authorized User eligible	2030 Add Auth User
Misc Field 10 Pos 1, External Status, Statement Hold Flag, # of Plastics	Misc Field 10 Position 1 is Z External Status of " " (blank) Internal Status of " " (blank) or "N" NOT Statement Hold Code of "R" NOT Auth Flag of "A" NOT # of Plastics of "0"	B3 Direct Bill Pay eligible	2340 Bill Payee 2400 Make Bill Payment
CVC	= CVC provided by Card Member	B1 CVC Enroll eligible	2480 Validate CVC

6.2.4 E-Mail Notifications

The following table provides a complete list of e-mails with definition of when e-mail gets generated, what dynamic content is included, and which addresses the e-mail is sent to.

ALERT	DYNAMIC COMPONENTS	LINKS	TRIGGER	TO:
Secure Message Reply	CM E-Mail Address CM First Name	Sign-In Sign-In	CSR User replies to Message	Profile Address

		w/automatic re-direct to Message Center tab		
Convenience Checks Requested	CM E-Mail Address CM First Name	Sign-In	Card Member requests Convenience Checks	Profile Address
Profile Changed	CM E-Mail Address CM First Name	Sign-In	Card Member changes profile	Profile Addresss
E-mail Address Changed	CM E-Mail Address CM First Name	Sign-In	Card Member changes profile	Profile Addresss Old E-mail Address
Statement Available	CM E-Mail Address CM First Name	Sign-In Sign-In w/re-direct to Statements tab Sign-In w/automatic re-direct to Alerts tab	System uploads statement data from MSR file	Alert Address OR Profile Address
Payment Past Due	CM E-Mail Address CM First Name	Sign-In Sign-In w/re-direct to Statements tab Sign-In w/automatic re-direct to Pay tab	System determines that payment is past due	Alert Address OR Profile Address
Payment Due in X Days	CM E-Mail Address CM First Name Payment Due Date	Sign-In Sign-In w/automatic re-direct to Pay Tab	System determines that payment is due in X days	Alert Address OR Profile Address
Credit Limit Reached	CM E-Mail Address CM First Name CM Credit Limit	Sign-In Sign-In w/automatic re-direct to Quick Pay Tab Sign-In w/automatic re-direct to Alerts tab	System determines that limit is reached	Alert Address OR Profile Address
Balance Within	CM E-Mail Address CM First Name Alert $ Amount	Sign-In Sign-In w/automatic re-	System determines that balance is within	Alert Address OR

		direct to Quick Pay Tab Sign-In w/automatic re-direct to Alerts tab	$X of credit limit	Profile Address
Balance Exceeds	CM E-Mail Address CM First Name Alert $ Amount	Sign-In Sign-In w/automatic re-direct to Quick Pay Tab Sign-In w/automatic re-direct to Alerts tab	System determines that balance exceeds $X	Alert Address OR Profile Address
Balance Drops Below	CM E-Mail Address CM First Name Alert $ Amount	Sign-In Sign-In w/automatic re-direct to Alerts tab	System determines that balance drops below $X	Alert Address OR Profile Address
Payment Applied	CM E-Mail Address CM First Name	Sign-In Sign-In w/automatic re-direct to Alerts tab	System determines that Payment posted by FDR	Alert Address OR Profile Address
Credit/Return Applied to Account	CM E-Mail Address CM First Name	Sign-In Sign-In w/automatic re-direct to Alerts tab	System determines that credit posted by FDR	Alert Address OR Profile Address
Purchase Item Exceeds	CM E-Mail Address CM First Name Alert $ Amount	Sign-In Sign-In w/automatic re-direct to Alerts tab	System determines that a purchase exceeds $X	Alert Address OR Profile Address
Enrollment completed	CM E-Mail Address CM First Name	Sign-In	System enrolls user	Profile Address
Payment Submitted	CM E-Mail Address CM First Name	Sign-In Sign-In w/automatic re-direct to Payment History tab	System creates a payment request	Profile Address
Direct Bill Payment Submitted	CM E-Mail Address CM First Name	Sign-In Sign-In	System creates a balance transfer	Profile Address

		w/automatic re-direct to Direct Bill Payment tab	request to make a Direct Bill Payment	