Discover Payment Services

CPP Fraud Services
Software Architecture Document

Version 1.0

Revision History

Date	Version	Description	Author
03/MAR/2017	Draft.1	Initial view of top-level system context.	Mike Knauff
21/MAR/2017	Draft.2	Added the following logical process diagrams: • Fraud Scoring • Case and Fraud Rules Management • Cardholder Profile Management	Mike Knauff
27/MAR/2017	Draft.3	Added the following logical process diagrams: • Fraud Rules Simulation	Mike Knauff
04/APR/2017	Draft.4	Added the following diagram: • Fraud Scoring Deployment Updated the following diagram • Fraud Rules Simulation	Mike Knauff
07/APR/2017	Draft.5	Updated all sections	Mike Knauff
10/APR/2017	1.0	Completed all sections and updated with feedback from FICO, Discover Cybersecurity, and BT Fraud	Mike Knauff

Table of Contents

Software Architecture Document

1. Introduction

1.1 Purpose

This document provides a comprehensive architectural overview of the system, using a number of different architectural views to depict different aspects of the system. It is intended to capture and convey the significant architectural decisions which have been made on the system. It is not intended as a detailed design document.

1.2 Scope

The CPP Fraud Services Software Architecture Document is intended to be used as a roadmap and guide for the design and implementation of the CPP Fraud Services, which is based upon the FICO Falcon product.

1.3 Definitions, Acronyms, and Abbreviations

1.3.1 Alert

An *Alert* is message that is sent to a financial institution or an fraud operations individual notifying them that a suspected fraudulent transaction was either blocked/declined by the system or that the transaction was forwarded to the financial intuition for authorization but that is was scored as suspected fraud.

1.3.2 ATM

Automated Teller Machine

1.3.3 CCM

CCM is the Falcon *Card Compromise Manager* that provides point-of-compromise analysis and detection.

Formatted: Body Text

1.3.4 CCS

CCS is the FICO provided and hosted *Customer Communication Services* that provides notifications to cardholders (customers) when the Falcon Fraud Scoring Engine detects a potentially fraudulent or risky transaction that the customer should be notified.

1.3.5 CHS

Cardholder (Account) Services is the new CPP application that is used to ingest and manage cardholder account data from financial institutions and issuers. This data is used to enrich fraud scoring and potentially other issuer-oriented products and services.

1.3.6 Client

A *Client* is the owner of the Falcon product installation and that is using the Falcon product to detect fraudulent transactions. Falcon *Clients* are identified by a Client ID within the Falcon system.

1.3.7 CRUD

CRUD is an acronym for common data operations: Create, Read, Update, and Delete.

1.3.8 Customer

A Falcon *Customer* is an identified cardholder within the Falcon system. Falcon *Customers* are identified by a Customer ID within the Falcon system.

1.3.9 FRM

FRM is the acronym for *Fraud Resolution Manager*, which is part of FICO's CCS product that provides real-time interaction with Falcon Customers via notifications regarding high-risk transactions.

1.3.10 Hotlists

Hotlists are groups of items associated with suspect activity within the Falcon system. *Hotlists* are defined by the Falcon Client and include items such as the following:

- High risk accounts and geographic areas
- Positive lists for VIP accounts
- Negative lists for suspect merchants, devices (ATMs), or customers

Hotlists are used by the Falcon Scoring Engine to help identify high-risk transactions.

1.3.11 Multi-Tenancy

Multi-Tenancy in the Falcon product is defined by the following hierarchy:

- Tenant = one of the Discover Payment Brands/Networks, and that is identified by separate Falcon Client IDs
- Sub-Tenant = a financial institution that has a fraud processing relationship with a Falcon Tenant

1.3.12 ms

Milliseconds

1.3.13 NAS

NAS is the acronym for *Network Attached Storage*.

1.3.14 Notification

A *Notification* is synonymous with an Alert but may also carry an additional meaning when related to customers. Customers may receive *notifications* of high-risk transactions via the FICO CCS service.

Formatted: Underline, Font color: Blue

1.3.15 SaaS

Software as a Service

1.3.16 SCCA

SCCA is the Falcon acronym for *Scoring Server Client Application*. The *SCCA* is a Client-provided component that provides the interface between the client's transaction authorization or routing platform and the Falcon Fraud Scoring server. The *SCCA* is responsible for providing any required communication protocol and message/data conversions between the client's transaction authorizer/switch and the Falcon Fraud Scoring Service.

1.3.17 tps

Transactions per second

1.3.18 User Defined Variables (UDV)

User Defined Variables (UDV) are Falcon parameters that are defined by the client and that keep track of calculation values or flags over time and across transaction types. Examples include the following:

- Count the volume of failed PIN transactions in the last 24 hours
- Store the data and time of the last address change
- Sum the value of transactions at Gas Stations in the last 3 days

UDV's are used by the Falcon Fraud Scoring Engine to help detect fraudulent transactions based upon variables that are defined by the client.

1.4 References

- Technical Notes from Houston Falcon Planning Sessions 28/FEB/2016 and 01/MAR/2016
- Falcon Design for Diners Club, Discover, and PULSE Networks
- Common Payments Platform Software Architecture Document
- Common Payments Platform Integrated Security Architecture Document

Formatted: No underline, Font color: Auto

- FICO Falcon Fraud for CPP/PULSE (Oracle Design)

1.5 Overview

The document is organized into the following major sections"

- *Architectural Representation* – provides a top-level context view of the system and the agents acting on the system or agents that are acted upon by the system
- *Architectural Quality Requirements* – the major goals of the architecture in terms of qualities such as availability and security
- *Size and Performance Requirements* – the major influences on the system architecture from a size and performance perspective
- *Constraints on the Architecture* – factors placing limitations on the architecture such as existing platforms, use of vendor products, time, etc.
- *Use-Case View* – provides the architecturally-significant use cases that provide the major drivers of the design of the architecture
- *Logical View* – provides an overview of the major functional and supporting components of the system
- *Process View* – documents how the components of the system interact dynamically to implement the major capabilities of the system
- *Deployment View* – provides a high-level view of how the components are deployed to release major qualities of the system such as availability and security

Formatted: Body Text, Keep with next

Formatted: Font: Italic

Formatted: Body Text, Bulleted + Level: 1 + Aligned at: 0.75" + Indent at: 1"

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Body Text

2. Architectural Representation

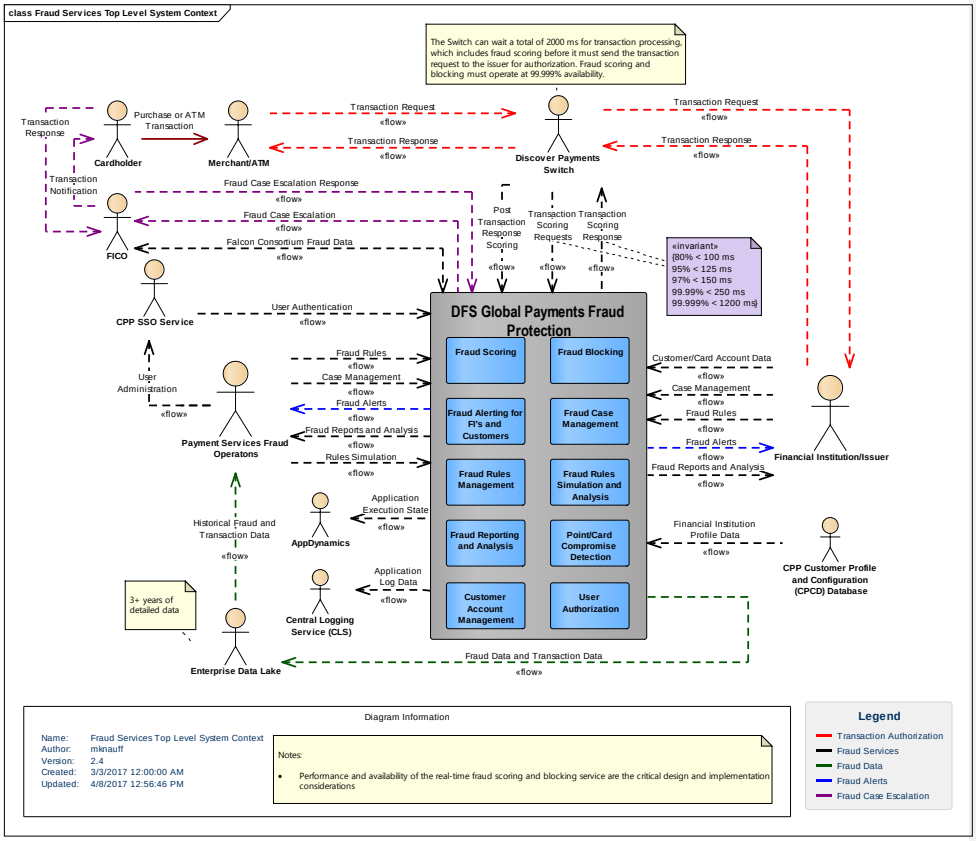

Figure 1. Fraud Services Top-Level System Context

2.1 Actors on the System (dependencies)

2.1.1 AppDynamics

AppDynamics monitors the state of the system components as well as the flow of service requests across system components and provides this information via a user interface to interested parties.

2.1.2 Cardholder (customer)

The *Cardholder* makes purchases or creates ATM transactions, which are scored for potential fraud and may receive transaction alerts for more information (fraud case escalation) in situations where the fraud scoring engine needs more information to make a determination of fraud.

2.1.3 Central Logging Service (CLS)

The *Central Logging Service (CLS)* captures the logging output (standard output and standard error) and routes these to a centralized repository, placed into a common format, and indexed for retrieval. The log data maybe queried and displayed via a CLS-provided UI. The log data in the CLS is used for security auditing, application warnings and alerts, and application diagnostics.

2.1.4 CPP Customer Profile and Configuration Data Base (CPCD)

The *CPCD* contains the party (financial institutions) profile data for fraud processing and unique identifiers that can be mapped to the Falcon Client ID's.

2.1.5 CPP SSO Service

The *CPP SSO Service* is responsible for both administering and storing user credentials, and providing authentication of both internal users (fraud operations) and external users (financial institution users) that request access to fraud resources through the pulsenetwork.com portal.

2.1.6 Discover Payments Switch

The *Discover Payments Switch* is responsible for routing transaction authorization requests and responses between merchants and issuers via their processors, and for blocking (declining) fraudulent transactions when appropriate. The *Discover Payments Switch* invokes the fraud scoring service in the following ways:

- Real-time/Score and Block (prior to transaction authorization – waits for the fraud score)
    - Invokes the fraud scoring service prior to sending the transaction for authorization to the issuer
    - Blocks the transaction and declines it if the fraud scoring service scores the transaction above a specific fraud threshold
    - The Alerting Service sends an alert to the issuer if the transaction was blocked due to fraud
- On-line/Score and Alert (during transaction authorization – fire and forget)
    - Invokes the fraud scoring service
    - The Alerting Service send an alert to the issuer if the fraud score is over a specific threshold
- On-line/Issuer Response (post authorization)
    - Invokes the fraud scoring service post authorization to enrich the previously scored authorization request with the issuer's response data

2.1.7 Enterprise Data Lake

The *Enterprise Data Lake* is responsible for receiving the fraud scoring data in near-real time, providing the historical repository of fraud scoring and transaction data, and providing access to the data for analysis by the Payment Services Fraud Operations.

2.1.8 FICO

FICO is the vendor that provides fraud alerts and case escalation services for contact with financial institutions (fraud alerts) and cardholders (fraud case escalation and notifications) in a SaaS model.

2.1.9 Financial Institution/Issuer

The *Financial Institution/Issuer* is the party that subscribes to the DFS Global Payments Fraud Protection Service for fraud rules management, fraud scoring, fraud alerts, fraud case management, etc. The *Financial Institution/Issuer* provides the payment accounts and devices to cardholders for the purpose of executing payment transactions, which run the risk of fraud under varying conditions.

2.1.10 Merchant/ATM

The *Merchant* or *ATM* is the accepting entity of the payment transaction that is unknown to the Financial Institution or Issuer and that accepts the payment transaction from a customer or cardholder that may be unknown to them. Fraud may be committed by the cardholder, the merchant, or malware that is a party to the transaction. The DFS Global Payments Fraud Protection Service is intended to mitigate the potential for fraud from these unknown relationships.

2.1.11 Payment Services Fraud Operations

Payment Services Fraud Operations is the DFS group responsible for monitoring and controlling fraud risk via the DFS Global Payments Fraud Protection Service platform. This group's primary responsibilities include management of fraud rules, fraud case management, fraud analysis, point of compromise detection, simulation and analysis of new fraud rules, etc.

2.2 DFS Global Payments Fraud Protection Services (fraud system)

2.2.1 Cardholder/Customer Account Management

The *Cardholder/Customer Account Management* Service provide the ability to ingest, store, and manage profile data that is specific to a customer and that is used by the fraud scoring engine to evaluate the fraud risk of a transaction or that is used by the Fraud Alerting Service to contact a customer when more information is needed from them in evaluating the fraud risk of a transaction (fraud case escalation).

2.2.2 Fraud Alerting for FI's and Cardholders/Customers

The *Fraud Alerting for FI's and Cardholders/Customers (Fraud Alerting)* Service provides the ability for the system to inform FI's in near-real time that a fraudulent transaction may have occurred and that some follow-up (fraud case management) is warranted. This service also can contact customers in near-real time via a preferred contact channel (phone – voice, phone – SMS, email) that a transaction on their account has occurred that contains additional risk factors. The customer may just want an alert or the system may ask for a follow-up action to confirm that the transaction was valid.

2.2.3 Fraud Blocking

The *Fraud Blocking* Service provides the ability for the Discover Payments Switch to receive a fraud score from the Fraud Scoring Service and then block/decline the transaction based upon the blocking threshold set for the fraud score range.

2.2.4 Fraud Case Management

The *Fraud Case Management* Service allows the users and the Fraud Scoring Service to create a fraud case that can be investigated and worked by either a Payments Services Fraud Operations User or a Financial Institution/Issuer User. The service provides a UI accessed via the SSO portal for the creation, viewing, and updating of suspected fraud cases.

2.2.5 Fraud Reporting and Analysis

Fraud Reporting and Analysis provides pre-defined reports false positives on accounts, rules, work queues, score bands, as well as provides ad hoc reporting capability.

2.2.6 Fraud Rules Management

Fraud Rules Management provides the ability for users to create, read, update, and delete fraud rules, as well as deploy the fraud rules for the fraud scoring process.

2.2.7 Fraud Rules Simulation and Analysis

The *Fraud Rules Simulation and Analysis* allows users to run new rules on production data and analyze their effect on transaction scoring. The simulation environment is a partial Falcon configuration that is deployed with the production environment but does not affect the production system.

2.2.8 Fraud Scoring

The *Fraud Scoring* Service provides the ability to utilize a number of factors such as vendor provided fraud models, card account hotlists, cardholder profile data, etc. to score payment transactions as to the likelihood that they are fraudulent. The *Fraud Scoring* Service provides the following capabilities:

- Real-time/Score and Block (prior to transaction authorization – waits for the fraud score)
  - Blocks the transaction and declines it if the fraud scoring service scores the transaction above a specific fraud threshold
  - The Alerting Service sends an alert to the issuer if the transaction was blocked due to fraud
- On-line/Score and Alert (during transaction authorization – fire and forget)
  - The Alerting Service sends an alert to the issuer if the fraud score is over a specific threshold
- On-line/Issuer Response (post authorization)
  - Enriches a previously scored authorization request with the issuer's response data

2.2.9 Point/Card Compromise Detection

The *Point/Card Compromise Detection* Service provides the ability to locate a likely merchant or ATM that has been compromised due to groups of fraudulent and/or uncharacteristic transactions being detected at that location by the system.

2.2.10 User Authorization

The *User Authorization* Service provides the ability to assign access privileges to specific system resources and for the system and to verify that a user has the proper access privilege before granting access to a system resource.

2.3 Strategic Roadmap

The initial implementation of the will be a PULSE-only implementation that will replace the current Retail Decisions (ReD) Debit Protect application, which goes out of support at the end of 2018. The initial PULSE roll-out will be primarily a "like-for-like" replacement of the ReD application. Future enhancements include the following:

- Addition of the FICO Falcon CCS services for transaction notifications and fraud alerts to customers (cardholders) and financial institutions
- Addition of the FICO Falcon CCM service for point-of-compromise analysis and detection
- Addition of cardholder demographic data to the fraud scoring process for more accurate fraud scoring capabilities based upon personal cardholder profile data
- Integration of Falcon Fraud detection and prevention capabilities into the Diners Club and Discover Networks

Formatted: Bulleted + Level: 1 + Aligned at: 0.75" + Indent at: 1"

3. Architectural Quality Requirements

3.1 Availability by Fraud Service

3.1.1 Real-Time (Authorization) Fraud Scoring

- 99.999% availability

3.1.2 Near-Real Time (Post Authorization) Fraud Scoring

- 99.9% availability

3.1.3 Batch Non-Mon Fraud Scoring

- 99.8% availability

3.1.4 Real-Time Fraud Blocks with Notification

- 99.999% availability

3.1.5 Near Real-Time Fraud Alerts with Notification

- 99.9% availability

3.1.6 Case Management

- 99.9% availability

3.1.7 Fraud Rules Management

- 99.9% availability

3.2 Security

3.2.1 Single Sign-On (SSO)

All user interfaces (internal and external facing) will be secured via an SSO service and the SSO service will be segmented by internal and external facing channels.

- Fraud Case Management
- Fraud Rules Management
- Fraud Reports and Analysis
- Customer/Cardholder Account Administration

3.2.2 User Authorization

User access to all fraud services will be secured via both course-grained and fine-grained access control. Course-grained authorization will be provided by the SSO service and fine grained access control by the fraud services.

3.2.3 System-to-System API Authentication and Authorization

3.2.3.1 External: Inbound to Discover from FICO

External API calls that are inbound to Discover from FICO-hosted services will utilize the Discover Layer 7 API Broker, which utilizes OAuth to authenticate the external system or entity and provides course-grained authorization for invoking the internally-hosted service.

3.2.3.2 External: Outbound from Discover to FICO

External API calls that are outbound from a Discover-hosted service (including Falcon services) will utilize either the OAuth or JWT standard for system authentication and course-grained authorization of the service call.

3.2.3.3 Internal

Internal API calls will utilize the Layer 7 API Broker and the JWT standard for system authentication and course-grained authorization of the service call. Service calls between Falcon components will be exempt from this requirement because vendor-provided services that do not conform to DFS standards but will be placed in DFS PCI-hardened security zones as a compensating control.

3.2.4 Channel Encryption

All external and internal service channels (http) will be encrypted (https) utilizing Transport Layer Security (TLS). The exchange of all external and internal files will utilize the Secure File Transfer Protocol (SFTP) over the Secure Shell (SSH).

Internal database access will utilize JDBC over TLS (jdbc/s) when the data is not hashed or encrypted within the communication channel.

3.2.5 Payload Encryption

3.2.5.1 REST Services

External REST service calls will utilize the JSON Web Encryption Standard to encrypt PCI-sensitive data (Content Encryption Key (CEK) and Key Encryption Key (KEK)).

Internal REST service calls will utilize the patterns and standards outlined in the Common Payments Platform Integrated Security Architecture Document for tokenizing/obfuscating PCI-sensitive data within the JSON payloads. The FICO Falcon product service calls will not conform to CPP security standards but will reside within DFS PCI-hardened security zones as a compensating control.

3.2.5.2 File Transfers

Internal and External file transfers will utilize the Discover file transfer manager, DFTP. DFTP supports payload encryption utilizing PGP for external file transfers. DFTP also authenticates and authorizes access to file transfer resources.

3.2.6 Data at Rest

3.2.6.1 Oracle – not Discover Standard (need follow-up)

- Oracle TDE or Oracle Tablespace Encryption will be utilized to encrypt PCI-sensitive data within the Oracle system
- Data Retention: 90 days for transaction data

3.2.6.2 Falcon Couchbase

- Falcon hashes the PAN data within Couchbase utilizing SHA-256 with salt

3.2.6.3 DFTP

- Gazzang AES 256 encryption

3.2.7 Data Risk

3.2.7.1 Critical Risk Data

- Most fraud services - PAN data

3.2.7.2 High Risk Data

- FICO Customer Contact Service (CCS) and CPP Cardholder Services
  - Customer Contact Information
    - Name
    - Address

- Array of phone number types (home, mobile, work, etc.)
  - Phone Number – voice notifications
  - Phone Number (mobile) – SMS notifications
  - Email address – email notifications

4. Size and Performance

4.1 Size

4.1.1 Average Daily Transaction[1] Volume Estimates

4.1.1.1 PULSE

- ≈ 10 MM

4.1.1.2 Diners Club

- ≈ 120 K

4.1.1.3 Discover

- ≈ 6 MM

4.1.2 Average Transaction Size Estimates

4.1.2.1 PULSE FINIPC

- 3.5 KB

4.1.2.2 Diners Club and Discover

- 1 KB

4.2 Performance

4.2.1 Transaction Processing Performance

The Falcon fraud scoring service will process 100% of the transaction authorization requests and responses. The Falcon fraud scoring engine will need to handle the following peak transaction scoring requests:

- 750 tps (all scoring – real time and online)
- 550 tps (real time only)

4.2.2 Response Latency Thresholds

The following are the latency thresholds that the PULSE Switch requires in order to score real-time transactions and not affect the performance of the switch and/or allow transactions to be sent to issuers without a fraud score[2]

- Tier 1 (< 100ms) 80%
- Tier 2 (< 125ms) 95%
- Tier 3 (< 150ms) 97%
- Tier 4 (< 250ms) 99.99%[3]
- Tier 5 (< 1200ms) 99.999%

[1] Includes a complete authorization transaction request-response pair as one (1) transaction

[2] The PULSE Switch will time-out the fraud scoring request after 1500 ms

[3] The PULSE Switch's performance begins to degrade as more transaction scoring responses approach 250 ms

5. Constraints on the Architecture

5.1 PULSE Switch Configuration

The *PULSE Switch* has two (2) geographically separated transaction switch clusters in the production environment:

- PRO1 located in the SSB
- PRO2 located in the ODC/BDC

Acquirers and issuer are sometimes connected to different instances in two data centers, which results for any given transaction that the acquirer may be connected to one (1) switch and the issuer is connected to the other switch. The transaction must be sent from one (1) switch to the other switch to complete the route to the issuer.

Formatted: Font: (Default) Times New Roman, Not Bold, Font color: Auto, Complex Script Font: Times New Roman, Not Bold

This configuration will prevent the Real-Time Fraud scoring service from running active-active in both centers and from being co-located with each switch cluster. An active-active configuration, co-located with each switch cluster would provide the optimum performance and availability configuration as fraud scoring requests could be kept local to each switch instance. However the *PULSE Switch* configuration will allow for only one (1) active instance of the real-time fraud scoring service that will allow only one of the switch clusters to make local scoring request and will force the other to make fraud scoring calls across the WAN causing greater latency and greater likelihood of service outages.

Achievable availability in the best case scenarios will be between 99.99% and 99.999% due to limitations in the implementations of some of the components such as FIS CONNEX, Oracle, Falcon Interface, and Falcon.

5.2 Time

The highest priority CPP Fraud Services must be ready for production and to start PULSE migration to the new fraud services by the end of 2nd Quarter, 2018. This will prevent all of desired fraud services from being implemented in the desired timeframe and may require trade-offs (goodness for time) during the construction and implementation phase, which may violate some of the architecture qualities and patterns.

5.3 Vendor Product

A vendor product, FICO's Falcon 6.x has been chosen to implement the majority of the CPP Fraud Services Platform. The physical architecture and implementation will be constrained by the capabilities of the product and the products technology stack.

6. Use-Case View

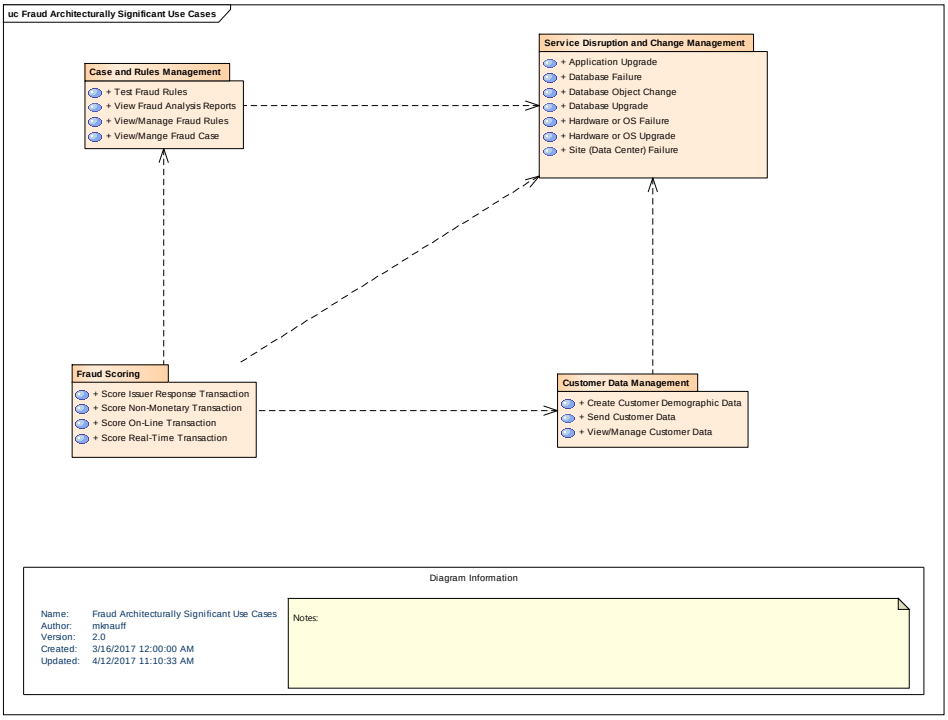

Figure 2. Architecturally-significant use-cases

6.1 Use-Case Realizations

6.1.1 Case and Rules Management

6.1.1.1 View/Manage Fraud Case

View/Manage Fraud Case allows issuers and fraud operations to view and update fraud cases created by the Fraud Scoring processes.

6.1.1.2 View/Manage Fraud Rules

View/Manage Fraud Rules fraud operations to create and update fraud rules and to deploy then for use by the Fraud Scoring processes.

6.1.1.3 View Fraud Analysis Reports

View Fraud Analysis Reports allows issuers and fraud operations to view statistics and metrics and fraud detection by the Falcon platform.

6.1.1.4 Test Fraud Rules

Test Fraud Rules allows fraud operations to update fraud rules and test them for false positives within a simulation environment that utilizes production data.

Formatted: Body Text

Formatted: No page break before

Formatted: Heading 4

Formatted: Font: Italic

Formatted: Body Text, Indent: Before: 1"

Formatted: Heading 4

Formatted: Font: Italic

Formatted: Body Text, Indent: Before: 1"

Formatted: Heading 4

Formatted: Body Text, Indent: Before: 1"

Formatted: Heading 4

Formatted: Body Text, Indent: Before: 1"

6.1.2 Scoring

6.1.2.1 Score Real-Time Transaction

Score Real-Time Transaction allows the system to score a transaction for fraud in-line of the authorization request, block/decline the transaction if it is = or > a specific threshold, and optionally send a fraud alert to the issuer.

6.1.2.2 Score On-Line Transaction

Score On-Line Transaction allows the system to score a transaction for fraud post authorization request and send a fraud alert to the issuer if it is = or > a specific threshold.

6.1.2.3 Score Issuer Response Transaction

Score Issuer Response Transaction allows the system to record an issuer's authorization response post authorization.

6.1.2.4 Score Non-Monetary Transaction

Score Non-Monetary Transaction allows the system to ingest non-monetary related data such as cardholder demographic data for enrichment of the fraud scoring process.

6.1.3 Customer Data Management

6.1.3.1 Create Customer Demographic Data

Create Customer Demographic Data allows issuers to submit cardholder demographic data that can be used in the fraud scoring process via file exchange, APIs, and/or browser UI applications.

6.1.3.2 View/Manage Customer Data

View/Manage Customer Data allows Discover operations and issuers to view and update cardholder account and demographic via a browser UI application.

6.1.3.3 Send Customer Data

Send Customer Data allows the cardholder account system to deliver cardholder demographic data to the fraud scoring system process via file transfer.

6.1.4 Service Disruption and Change Management

6.1.4.1 Application Upgrade

Application Upgrade allows the system to upgrade various applications involved in the fraud monitoring and prevention process and still maintain platform availability targets for critical and non-critical portions of the platform.

6.1.4.2 Database Failure

Database Failure allows the various platform databases to fail due to hardware, middleware, software, or corruption issuers and still maintain platform availability targets for critical and non-critical portions of the platform.

6.1.4.3 Database Object Change

Database Object Change allows the various platform databases to accept updates to the database structure and still maintain platform availability targets for critical and non-critical portions of the platform.

6.1.4.4 Database Upgrade

Database Upgrade allows the various platform databases to accept updates to the database software and still maintain platform availability targets for critical and non-critical portions of the platform.

Formatted: Font: Italic
Formatted: Indent: Before: 1"
Formatted: No page break before
Formatted: Font: Italic
Formatted: Body Text, Indent: Before: 1", No page break before
Formatted: Body Text, Indent: Before: 1"
Formatted: Body Text, Indent: Before: 1"
Formatted: Heading 4
Formatted: Font: Italic
Formatted: Body Text, Indent: Before: 1"
Formatted: Heading 4
Formatted: Font: Italic
Formatted: Body Text, Indent: Before: 1"
Formatted: Heading 4
Formatted: Body Text, Indent: Before: 1"
Formatted: Font: Italic
Formatted: Body Text, Indent: Before: 1"
Formatted: Body Text, Indent: Before: 1"
Formatted: Font: Italic
Formatted: Body Text, Indent: Before: 1"
Formatted: Font: Italic
Formatted: Body Text, Indent: Before: 1"

6.1.4.5 Hardware or OS Failure

Hardware or OS Failure allows the various platform hardware components to fail and still maintain platform availability targets for critical and non-critical portions of the platform.

Formatted: Font: Italic

Formatted: Body Text, Indent: Before: 1"

6.1.4.6 Hardware or OS Upgrade

Hardware or OS Upgrade allows the system to upgrade various hardware and OS software components involved in the fraud monitoring and prevention process and still maintain platform availability targets for critical and non-critical portions of the platform.

Formatted: Font: Italic

Formatted: Body Text, Indent: Before: 1"

6.1.4.7 Site (Data Center) Failure

Site (Data Center) Failure allows a complete site outage and still maintain fraud monitoring and prevention platform availability targets for critical and non-critical portions of the platform.

Formatted: Font: Italic

Formatted: Indent: Before: 1"

7. Logical View

7.1 Overview

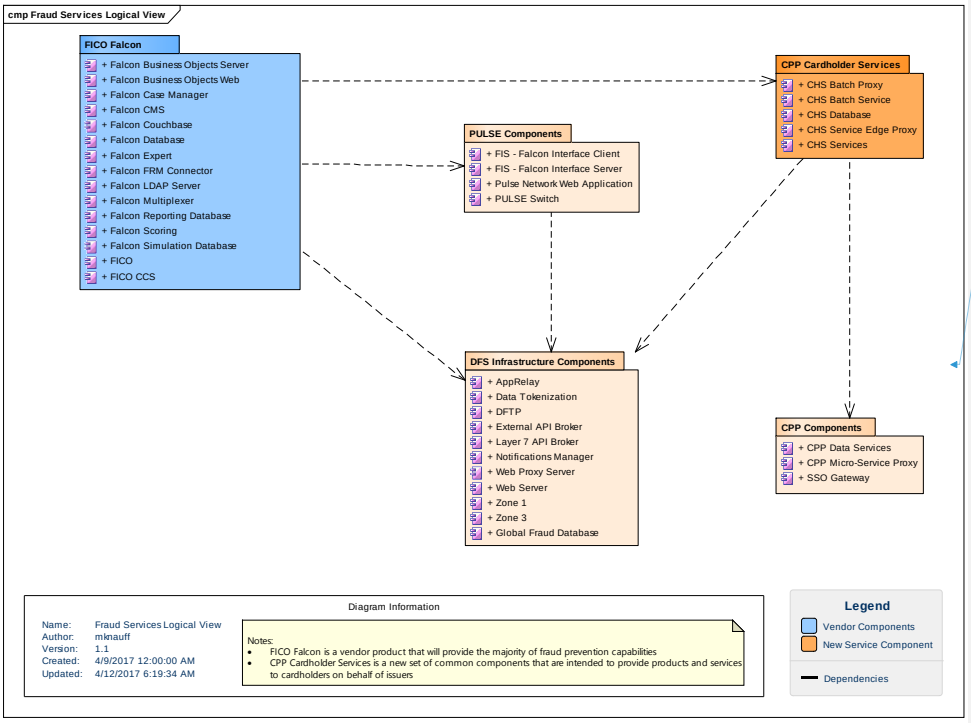

Figure 3. DFS Global Fraud Prevention Services Logical View

7.2 Architecturally Significant Design Packages

The following is the list of architecturally-significant component packages involved in the design solution.

7.2.1 CPP Cardholder Services

CPP Cardholder Services is a new Discover Common Payments Platform product that provides the ability to accept cardholder data such as account identifier, card products including PAN, contact information such as address, payment and contact device types (mobile, phone, tablet, laptop, etc.), contact numbers (mobile, home, work, etc.), and other demographic information. This information is used in fraud monitoring and scoring, cardholder alerts and notifications, as well as potentially other cardholder and issuer services.

Key components involved in this service include channel interfaces for Portal/UI, API, and batch files, processing and service components, as well as a persistent data repository.

Formatted: Body Text

7.2.2 CPP Components

The *CPP Components* provide reusable services for the new CPP Cardholder Services including customer[5] profile and configuration data and security services.

7.2.3 DFS Infrastructure Components

The *DFS Infrastructure Components* provide common services such as channel management (file transfers, APIs, Portal/UI), security, notifications, etc.

7.2.4 FICO Falcon

FICO Falcon is the vendor product that provides the bulk of fraud scoring, management, and monitoring services including fraud scoring, case management, rules management, reporting, etc.

7.2.5 PULSE Components

The *PULSE Components* provide the source and primary client of transaction scoring for fraud, the proprietary interface between the transaction source (PULSE Switch) and the Falcon Scoring servers, and the SSO service for users to gain access to the Falcon case and fraud management services, as well as fraud reporting.

[5] CPP customers are network or platform customers such as acquirers, issuers, processors, payment service providers, etc. and not cardholders from the CPP perspective.

8. Process View

8.1 Fraud Scoring

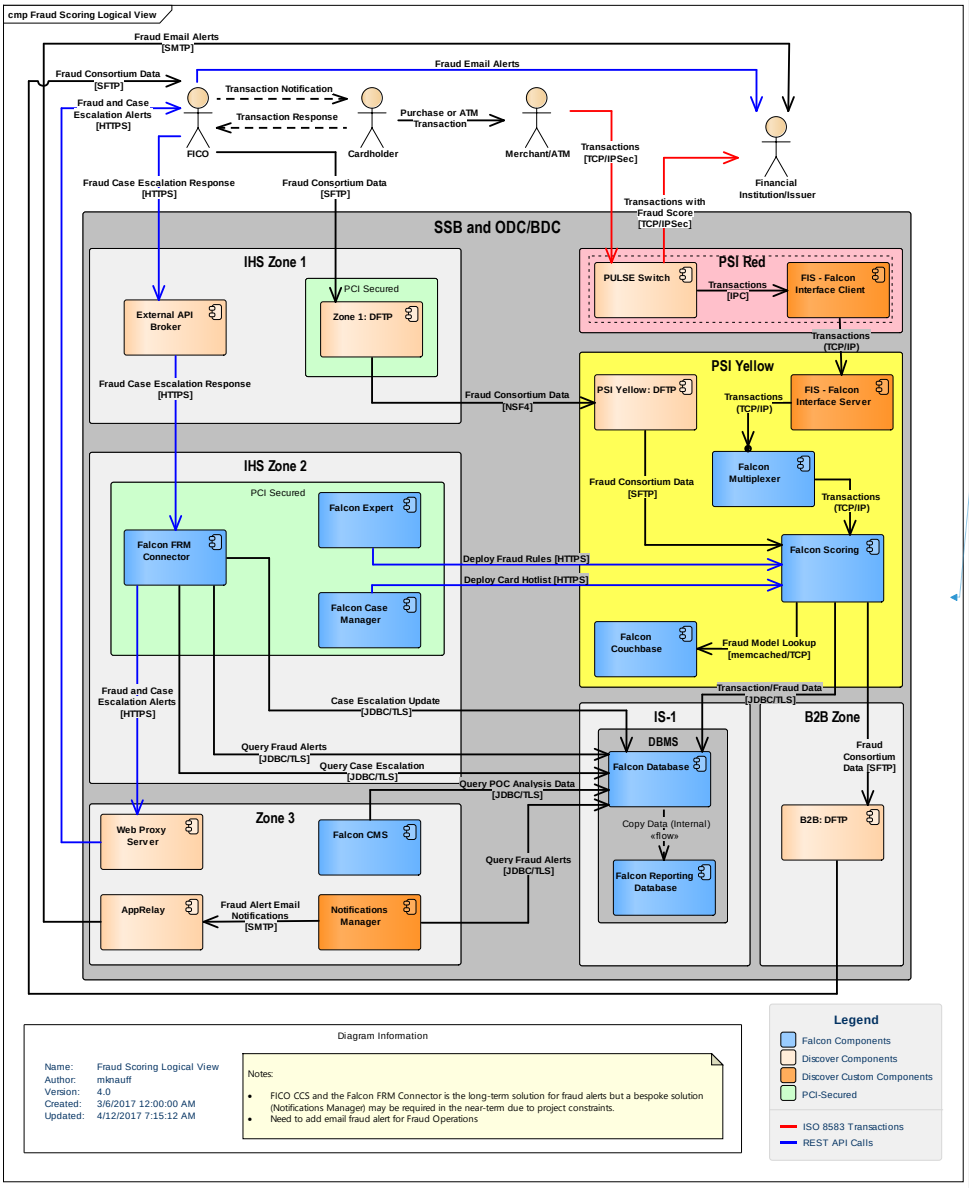

Figure 4. Falcon Fraud Scoring Logical View

Formatted: Body Text

8.1.1 Description

Falcon fraud scoring ingests transactions from the PULSE Switch via a bespoke interface (FIS – Falcon) Interface that converts the transaction message into the Falcon format and manages the interface with the Falcon Multiplexers.

The Falcon Multiplexers manage communication with multiple instances of the Falcon Scoring engines. The Falcon Scoring engines are dependent upon the low-latency Couchbase databases for look-ups of the appropriate fraud profile models for scoring of the transactions and any user-defined variables, reading and triggering of any fraud rules deployed by Falcon Expert, hotlists (card, device, etc.) deployed by Falcon Case Manager, and reading of customer demographic and cryptography salt values from the Falcon Database as well as asynchronous writes to the database of fraud case and transaction data. The Falcon Scoring engines also send to FICO and receive from FICO Falcon fraud consortium data files via the Discover DFTP platform.

Fraud notifications and alerts can be sent via two (2) potential channels:

- A Discover bespoke component called Notifications Manager that polls the Falcon Database looking for fraud notifications and alerts to send via email to Financial Institutions and Discover Fraud Operations
- A Falcon-provided SaaS service that utilizes a Falcon-provided interface (Falcon FRM Connector) that also queries the Falcon Database for notifications and alerts, and then sends these to the FICO SaaS service via a REST call for distribution to customers and Financial Institutions
    - Depending on the customer notification type (fraud case escalation) FICO may return additional data from a customer response regarding a fraud case, which is then updated in the Falcon Database

A process copies data from the Falcon Database to the Falcon Reporting Database so that fraud queries and reports can be executed without impacting the performance of Falcon Scoring operations on the Falcon Database.

8.2 Case and Fraud Rules Management

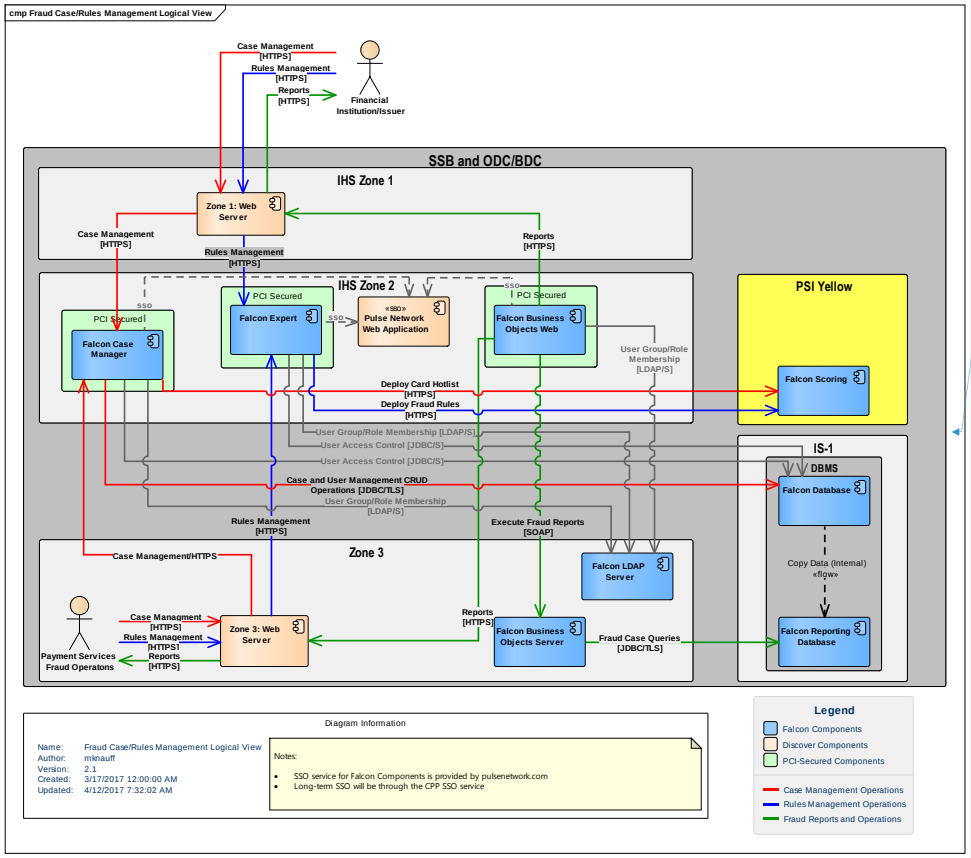

Figure 5. Falcon Case and Rules Management Logical View

8.2.1 Description

Internal and external users manage cases using Falcon Case Manager, create and manage fraud rules using Falcon Expert, and then review fraud and fraud analysis reports Falcon Business Objects Web. Access to these applications is managed by the PULSE Network Web Application via its proprietary SSO service for authentication of user credentials. The Falcon user components (Falcon Case Manager, Expert, and Business Objects Web) leverage the PULSE SSO service for user authentication and then determine user group/role membership (Falcon LDAP Server), and fine grained access control and authorization is stored within the Falcon Database. Falcon Case Manager is utilized for the administration of users, groups, roles, permissions, etc.

Falcon Case Manager performs CRUD operations on fraud case, hotlist, and fraud case work queues data stored within the Falcon Database. Falcon Case Manager deploys the various card and device hotlists to the Falcon Scoring servers via a REST service.

Formatted: Body Text

Falcon Expert performs CRUD operations on fraud rules stored within the Falcon Expert Rules Repository (implemented in NAS). Falcon Expert deploys the Fraud Rules via a REST service to the Falcon Scoring servers.

Fraud Reports are made available to users through Falcon Business Objects Web. Falcon Business Objects Server queries the Falcon Reporting Database to provide a variety fraud and fraud analysis reports.

8.3 Cardholder Profile Management

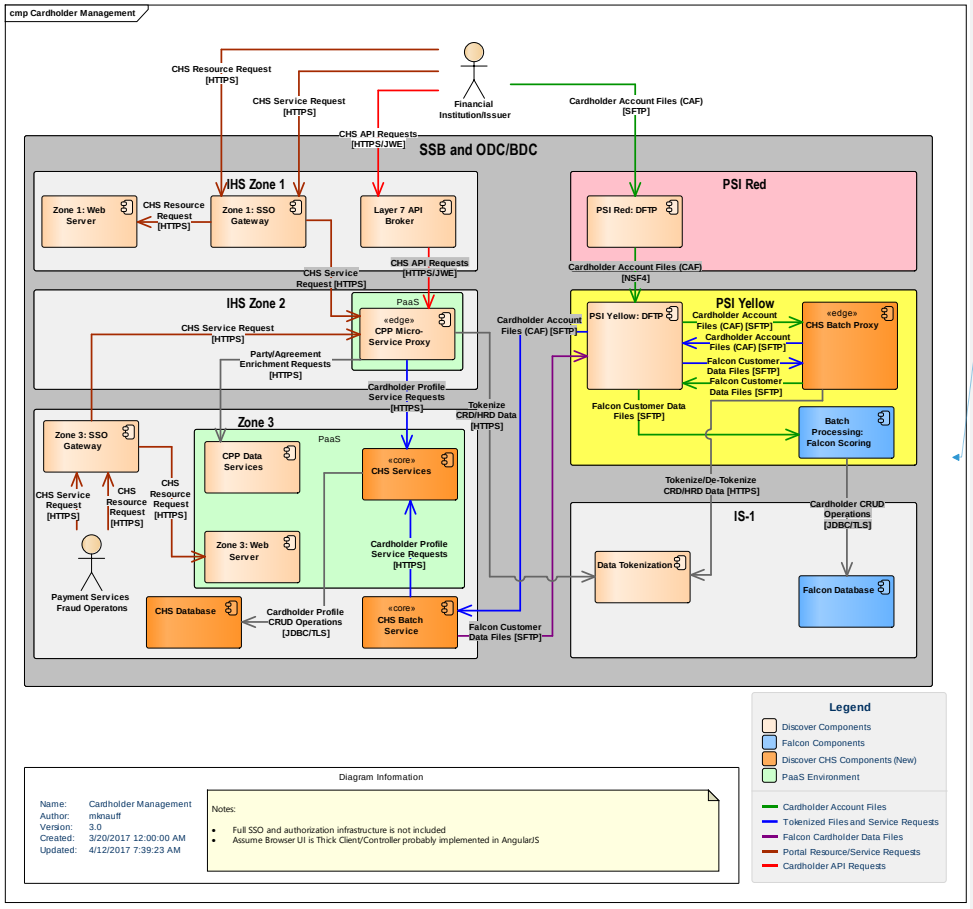

Figure 6. Cardholder Account Management Logical View

8.3.1 Description

The CHS follows the Common Payments Platform Software Architecture and the Common Payments Platform Integrated Security Architecture.

The CPP Cardholder Services (CHS) provides multiple channels for the creation and maintenance of cardholder accounts. The CHS provides UI/rich client access through the SSO Gateway for user authentication and the Web Server for the distribution of UI resources such as the required JavaScript code for creation and operation of the content and controller code on the browser client. The Layer 7 API Broker provides authentication and management of external API requests for CHS service requests. DFTP provides the authentication and management of cardholder account file transfers.

Formatted: Body Text

CHS browser service and API requests are managed by the CPP Micro-Service Proxy that provides a variety of security services for the requests including tokenizing CRD and HRD data, translation to the CPP canonical format, and enriching the requests with party and agreement data before invoking the requested CHS services.

File-based CHS service requests are managed by the CHS Batch Proxy, which performs a similar set of services for file data as the CPP Micro-Service Proxy does for service and API requests. CRD and HRD data is tokenized, the data is translated into the CPP canonical format, and the data is enriched with party and agreement metadata before being sent the CHS Batch Service for service processing. The CHS Batch Service performs the file processing and invokes CHS Services for application of the business logic and for operations on the CHS Database.

Falcon Customer Data that supplies the customer demographic data required by Falcon for more accurate fraud scoring is sent to the Falcon Batch Processing Scoring process by first extracting the appropriate demographic data elements from the CHS Database and then sending these to the CHS Batch Proxy for de-tokenization of the CRD and HRD data and translation from the canonical format and into the Falcon format. The CHS Batch Proxy sends the Falcon Customer Data File to the Falcon system via DFTP.

8.4 Fraud Rules Simulation

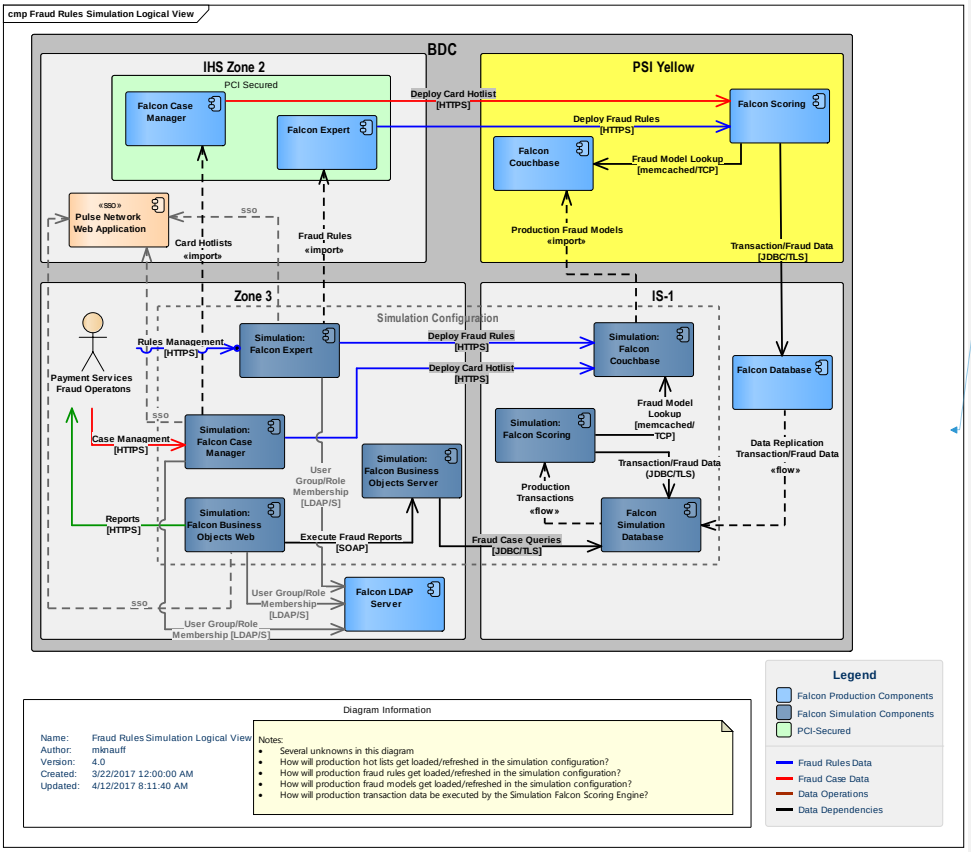

Figure 7. Fraud Rules Simulation Logical View

8.4.1 Description

FICO provides a rules simulation configuration within the production environment in order to run fraud rules on production data in order to look for false fraud positives and test changes to the fraud rules. The Falcon Simulation Configuration in the production environment mirrors the types of Falcon components that provide the actual production Falcon Fraud Scoring. The major differences are the following:

- All Falcon simulation components are located in Zone 3 and IS-1 since only the Payment Services Fraud Operations group needs access to these components
- The size and scale of these components are less than those that are performing the production fraud scoring

Key processes include:

- The copying of transaction and fraud case data from the Falcon Database in production and into the Falcon Simulation Database

Formatted: Body Text

- The copying of fraud rules from Falcon Expert in production and into Falcon Expert Simulation[6]
- The copying of hotlists from Falcon Case Manager in production and into Falcon Case Manager (via the Falcon Database copy process)
- The copying of the fraud models from Falcon Couchbase in production and into Falcon Couchbase Simulation

[6] The same NAS rules repository may be shared between the production and simulation configurations

9. Deployment View

9.1 Connectivity

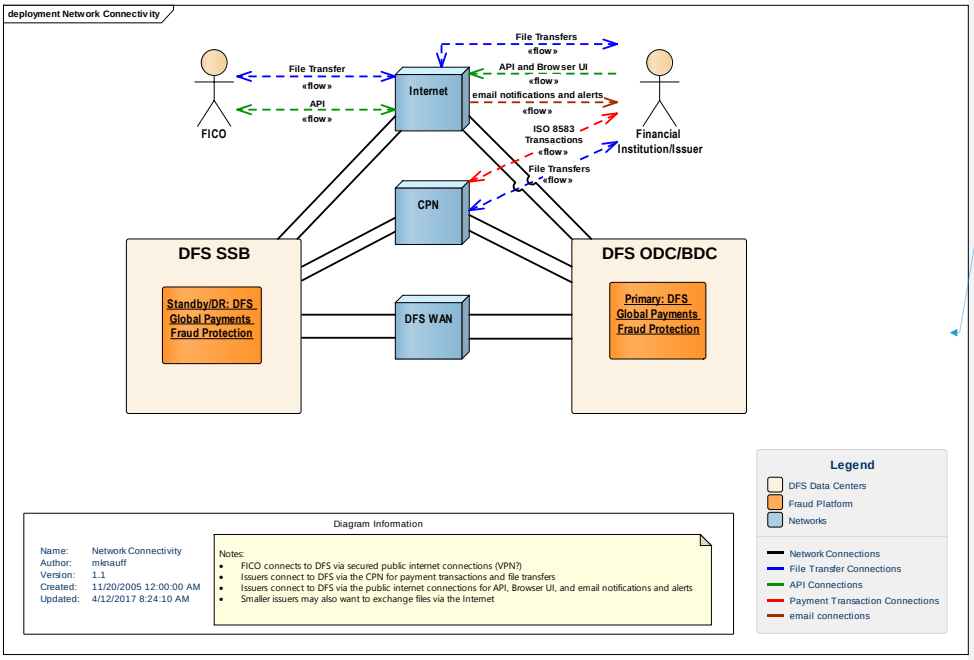

Figure 8. DFS Global Payments Fraud Platform Connectivity

9.1.1 Description

The DFS Global Payments Fraud Protection Platform runs active in one data center and is in a hot standby mode in the second center. Data between the two (2) systems is replicated in near-real time. Data Replication occurs across the DFS WAN via redundant connections.

FICO connects to DFS via secured Internet connections for the exchange of data files and for API calls. The file exchanges and API calls occur in both directions.

Financial institutions and issuers (or their processors) connect to DFS via the CPN network for the exchange of ISO 8583 Payment Transactions and the exchange of file transfers if they already have existing CPN connections with DFS. Smaller financial institutions and issuers that do not have pre-existing CPN connections with DFS will exchange data files related to the fraud service via secure internet connections. Financial institutions and issuers will also connect to DFS via the internet for direct access to fraud service APIs, use of the Fraud Services UI, and receipt of fraud case notification and alerts.

Formatted: Normal

9.2 Fraud Scoring

Formatted: Page break before

Formatted: Body Text

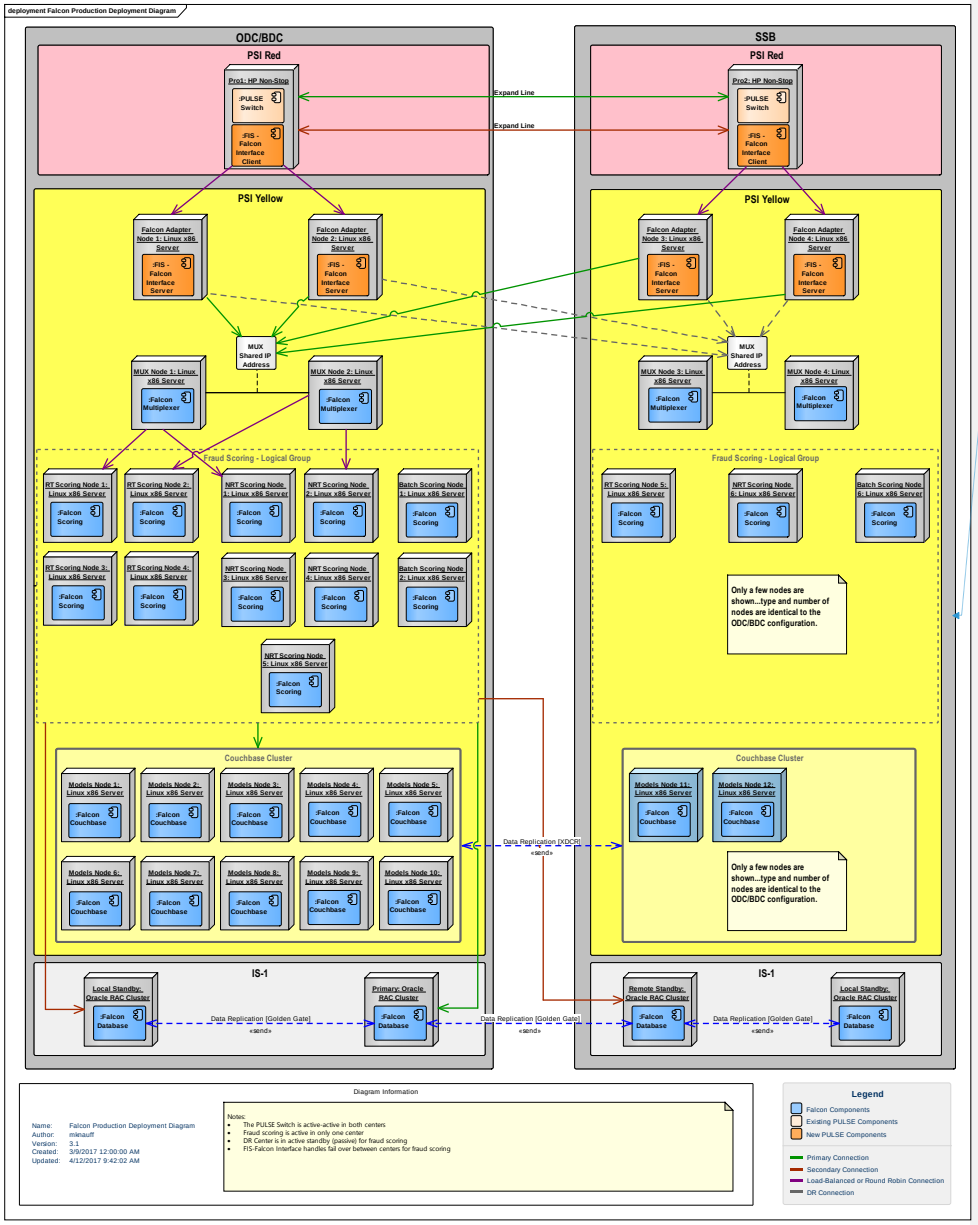

Figure 9. Fraud Scoring Deployment and Availability

9.2.1 Description

There are two (2) active instances of the PULSE Switch running in both the ODC/BDC and SSB. There are FIS – Falcon Interface Client processes that run on both switch servers. The client processes are responsible for transmitting transaction data to the FIS – Falcon Interface Server processes running on separate servers. The client processes round-robin or load balance fraud scoring requests between the server nodes.

The FIS – Falcon Interface Servers are responsible for translating the FIS FINIPC transaction format into the Falcon format and passing these requests to the Falcon Multiplexers for Fraud Scoring. The FIS – Falcon Interface Servers are responsible for managing the connections to the MUX as well as the exchange of fraud scoring requests and responses. All scoring requests are sent to a shared MUX IP address that the MUX servers manage for high availability.

The MUX servers are responsible for managing the fraud scoring requests and responses with the various fraud scoring servers. The MUX servers route real-time[7] fraud scoring requests to the real-time scoring servers for potential transaction blocking and near real-time fraud[8] scoring requests to the near real-time scoring servers for fraud alerting only or recording of the issuer's authorization response. There many instances of the fraud scoring servers for performance and to maintain high-availability.

The Fraud Scoring servers are dependent on the Oracle database for customer demographic data and for creating fraud cases and for storing transaction data. Data performance is maintained by a dedicated Oracle RAC cluster co-located with the active fraud scoring servers. High-Availability is maintained by the Oracle RAC cluster against single database server or node failures and by caching of the Oracle reads and writes by the Falcon Scoring servers, which can go up to 30 minutes with a database outage. Additional database availability is provided by a local dedicated standby Oracle RAC cluster in hot standby that allows the Fraud Scoring servers to be redirected to this cluster in case of a cluster failure of the primary cluster within 15 minutes of the failure of the primary cluster or for maintenance that needs to be performed on the primary Oracle RAC cluster. The Oracle RAC Clusters (primary and local standby) have data being replicated in real time utilizing Golden Gate and with both Oracle RAC clusters open for reads and writes, however writes only occur in one (1) direction at a time in order to manage the complexity of data synchronization. The Primary Oracle RAC cluster also replicates its data in real time to a remote standby Oracle RAC cluster in hot standby to protect against site outages due to a disaster or when Falcon maintenance requires the entire Falcon platform to be brought down on the primary location.

The Fraud Scoring servers are also dependent in real time for fraud model profile lookups on the Falcon Couchbase servers. High performance is maintained on these lookups using the memcached protocol and multiple instances within the cluster. High availability is maintained by the Couchbase cluster managing the many Couchbase nodes for failure protection and recovery.

9.2.1.1 Planned Maintenance

The entire platform is designed to maintain between 99.99% and 99.999% availability for planned maintenance. Maintenance of the PULSE Switch allows for processors to be gracefully moved from one instance to the other instance with fraud scoring requests continuing to flow to the primary fraud scoring platform through connections managed by the FIS-Falcon Interface.

Formatted: Heading 4

Formatted: Indent: Before: 1"

[7] Real-time scoring request are those that may result in blocking of the transaction at the switch, so these are performed "in-line" of the authorization request.

[8] Near real-time scoring requests are those that either may result in a fraud alert only to the issuer and are not performed in-line of the authorization request, or recording of the issuer authorization response, which occurs post-authorization.

Planned maintenance on the FIS-Falcon Interface may mirror the PULSE Switch maintenance model where all traffic is migrated to one switch instance allowing the FIS-Falcon upgrade to be performed and then migrating processor connections to be slowly migrated back to the upgraded instance and then following a similar process on the other switch instance. Depending on the sophistication of the FIS – Falcon Interface Client components a less invasive upgrade process could be supported for at least the FIS – Falcon Interface Server components, which would allow the Client components to be connected to Server components in the other data center during server component upgrades.

The Falcon component outages during upgrades or patching will depend on the nature of the upgrade or patch. FICO has indicated that most changes to the platform will require taking the entire platform out of operation in the primary center and switching to the DR location. Both FICO and FIS have indicated that it should be possible to gracefully take down the Falcon platform, i.e. redirect scoring requests to the DR platform and allow trailing requests to complete while switching over to the DR platform. This will require both Oracle RAC clusters, primary and remote standby, to be receiving write requests during the switch over process but replication only occurring from the primary cluster and to the DR cluster while the primary platform is shutting down. Management of the Golden Gate replication will be important during this process as the data that is being written to the DR copy during the switch-over will need to be written back to the primary RAC cluster once processing at the primary RAC cluster is restored.

Maintenance that affects only the primary Oracle RAC cluster will allow the primary Falcon platform to remain in operation while Falcon database connections are switched from the primary Oracle RAC cluster and to the local Oracle RAC standby cluster. Similar to the process for switching from the primary to remote standby RAC clusters, replication managed by Golden Gate will need to be carefully directed back and forth between the primary and local standby clusters.

9.2.1.2 Disasters

Disasters or unplanned outages to any of the individual PULSE Switch, FIS – Falcon Interface, Falcon, or Oracle components should be reasonably tolerant of these outages due to the use of multiple active copies and clustering or other high-availability patterns and technologies. The platform should be able to maintain 99.99% to 99.999% availability during minor unplanned outages. However cluster failures or site-level disasters will be more of a challenge to maintain availability targets. Challenges will exist at the FIS-Falcon Interface and Oracle level depending on the nature of the disaster and how automated the change-over from the primary site and to the DR site can occur. It is unknown at this time exactly how robust the FIS-Falcon Interface can be mode in terms of automating fail-over. The largest amount of time may be lost in communicating the disaster and giving permission to execute the fail-over scripts.

Formatted: Heading 4

Formatted: Indent: Before: 1"

Formatted: Heading 1