



December, 20 2010

Andrew Attebery
Innssoft
14355 SW Allen Blvd
Suite 240
Beaverton, OR 97005

Dear Andrew Attebery:

Our recent analysis of the NB. message format for authorization requests and settlement files you submitted via Internet Protocol Network (IPN) powered by Datawire, frame relay TCP/IP into the risc6000 interface, show your product to be within the file format guidelines for the First Data Commercial Services South platform.

File Format Specifications that were utilized:

FDMS South Platform Merchant Interface Specifications via Dial Up, NB. Terminal Capture Credit Card Authorization and Settlement Formats for Retail, Hotel Lodging, Restaurant, and Mail/Telephone Order; May 11, 2010 version 2010-1

This letter serves as notification that your Hotel Lodging product, **Check-Inn Credit version 5.0.0**, has been validated as compliant with the file format guidelines by First Data Commercial Services south platform.

The record format validation was successful and includes the following:

CONNECTIVITY	MARKET SEGMENT(S)	ENTITLEMENTS (CARD TYPES)	FEATURES / FUNCTIONALITY
Via Internet Protocol Network (IPN) powered by Datawire, Frame Relay TCP/IP into the risc6000 interface	Hotel Lodging	Visa, MasterCard, American Express, Discover*, Diners and JCB cards *including new Discover Bins	<ul style="list-style-type: none"> Track 2 Data Authorization and Settlement Supports American Express Special Program Codes 1, 2, and 3 Supports Hotel Lodging transaction only Swiped and Keyed/ Voice Auth/ Voids/ Refunds Supports minimum zip code on manually key entered transaction Supports Visa CVV2, MasterCard CVC2, American Express CID, and Discover CID Visa Incremental MasterCard Corporate, Commercial, Business and Corporate Purchasing Card Level III TPP ID VIS003

The card associations update their requirements periodically, generally twice per year. FDMS will issue updates to its format specifications from time to time, usually in conjunction with the card association revisions to their rules. All FDMS specification updates are available online at www.fdms.com. You should review this site for updates frequently. You will be required to update, retest and recertify your application as specifications are updated.

In addition to this FDMS validation, your POS products (all versions) must undergo and successfully complete a Payment Application Best Practices (PABP) data security standards audit by an approved PCI security assessor. Software vendors must ensure that all of their end-users (merchants) are fully updated to compliant versions of their POS products.

In the event that this software requires code changes, in order to maintain ongoing certification with current FDMS requirements and Card Association processing guidelines, you must re-certify with FDMS and re-validate with your PABP security assessor. Note, validation of compliance with PABP guidelines and Card Association requirements is not a guarantee against data security compromise and resulting liability. The PABP guidelines and Card Association requirements are subject to change periodically. It is each POS software vendor's responsibility to maintain compliance with the most current guidelines and requirements for their respective POS products.

If you have any questions or concerns, please feel free to contact us:

Business: Kathy Theiss FDMS Vendor Relations at 631-683-6326 – Kathy.Theiss@FirstData.com

Technical: Maria Martinez, Client Certification and Implementation Analyst at 954-845-4323 – Maria.Martinez@firstdata.com