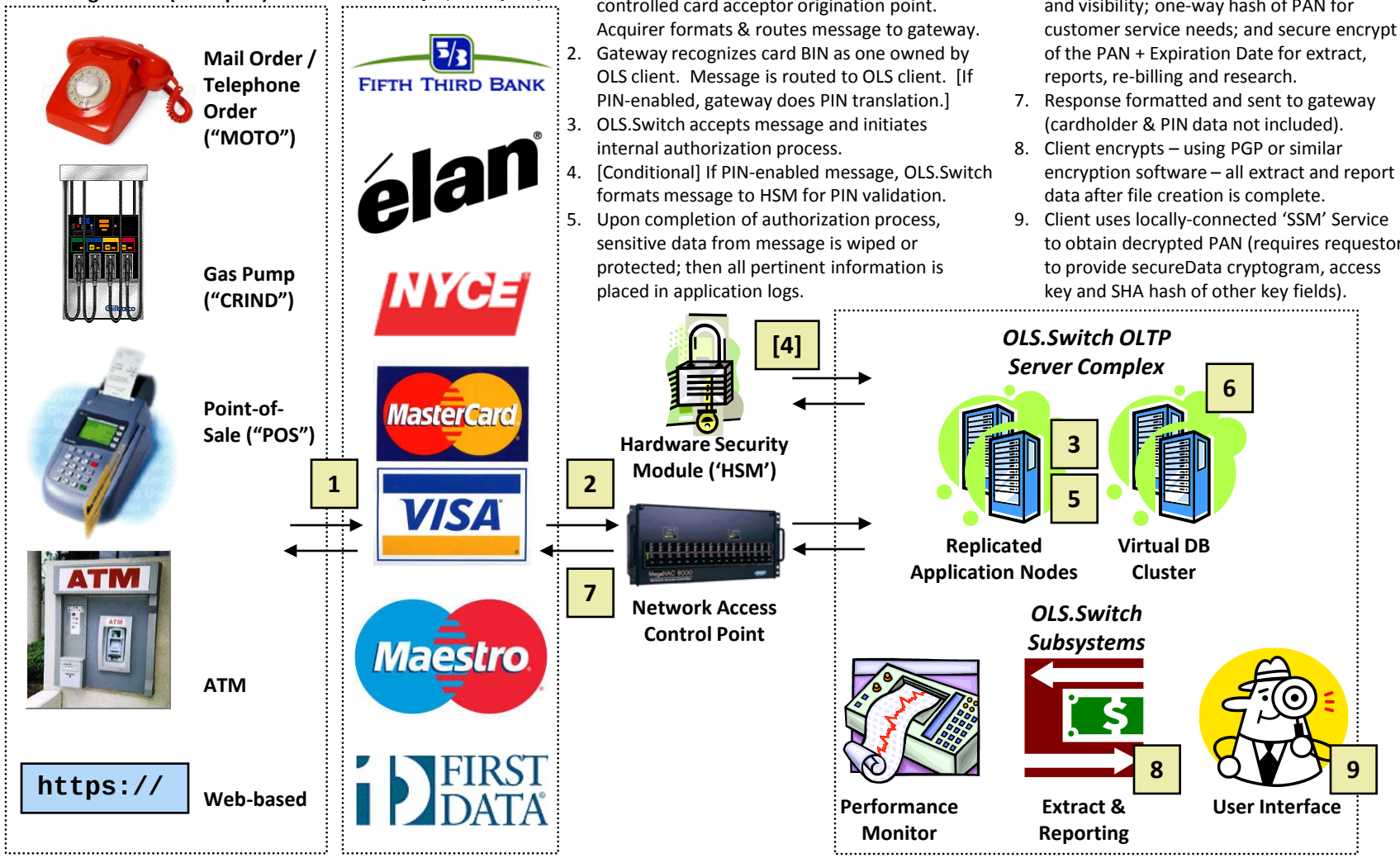
OLS.Switch Cardholder Data Flow (as Issuer)

1. Authorization request ('message') by OLS.Switch client's cardholder is initiated at acquirer-controlled card acceptor origination point. Acquirer formats & routes message to gateway.
2. Gateway recognizes card BIN as one owned by OLS client. Message is routed to OLS client. [If PIN-enabled, gateway does PIN translation.]
3. OLS.Switch accepts message and initiates internal authorization process.
4. [Conditional] If PIN-enabled message, OLS.Switch formats message to HSM for PIN validation.
5. Upon completion of authorization process, sensitive data from message is wiped or protected; then all pertinent information is placed in application logs.
6. Transaction is written to the transaction log; includes: truncated PAN for research 'hint' and visibility; one-way hash of PAN for customer service needs; and secure encrypt of the PAN + Expiration Date for extract, reports, re-billing and research.
7. Response formatted and sent to gateway (cardholder & PIN data not included).
8. Client encrypts – using PGP or similar encryption software – all extract and report data after file creation is complete.
9. Client uses locally-connected 'SSM' Service to obtain decrypted PAN (requires requestor to provide secureData cryptogram, access key and SHA hash of other key fields).



OLS, © 2008 – Confidential Material