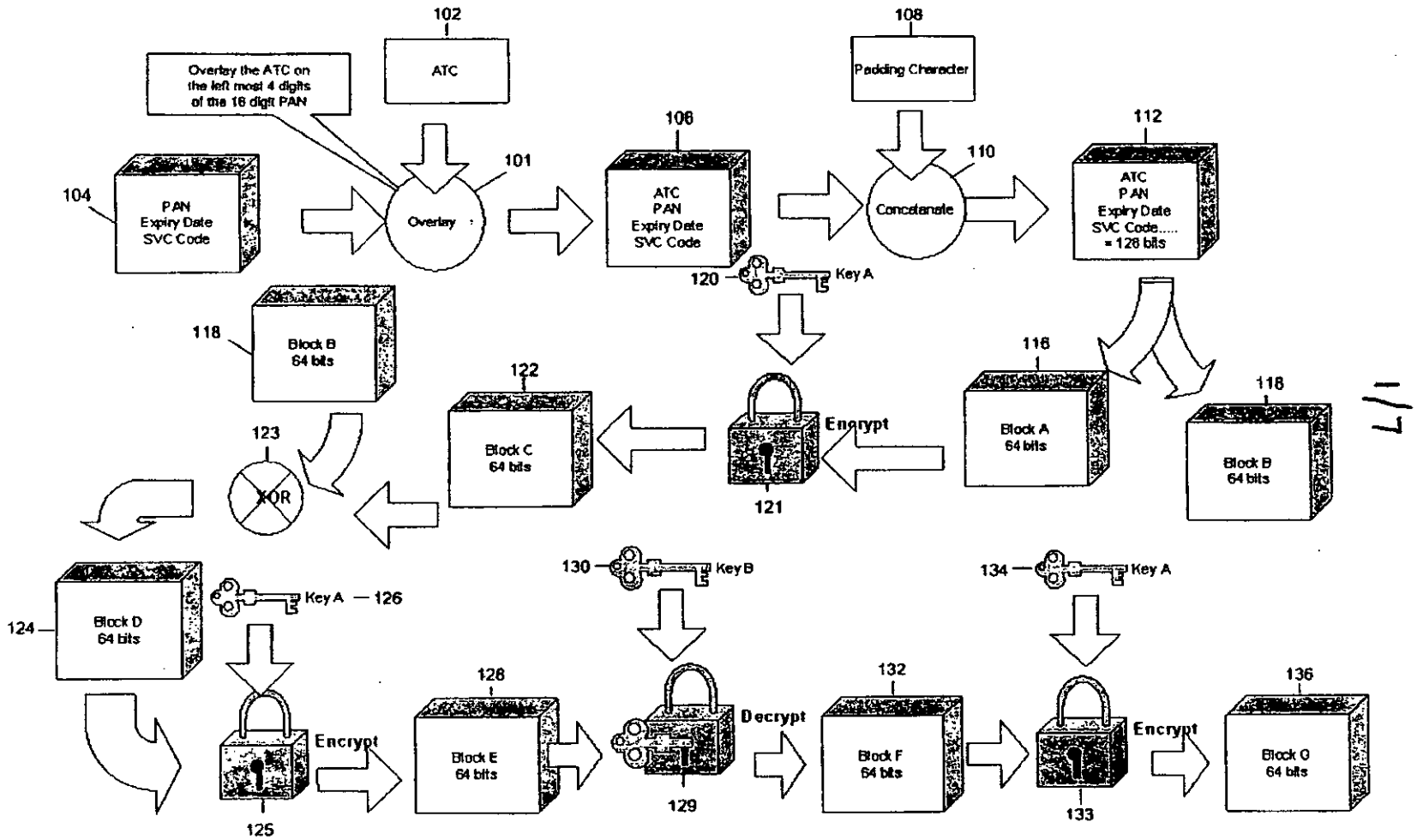

102
ATC
Overlay the ATC on the left most 4 digits of the 16 digit PAN
108
Padding Character
106
112
104
PAN Expiry Date SVC Code
101
Overlay
ATC PAN Expiry Date SVC Code
110
Concatenate
ATC PAN Expiry Date SVC Code..... = 128 bits
120
Key A
118
Block B 64 bits
116
Block A 64 bits
118
Block B 64 bits
122
Block C 64 bits
Encrypt
121
123
XOR
130
Key B
134
Key A
124
Block D 64 bits
Key A
126
Encrypt
125
128
Block E 64 bits
129
Decrypt
132
Block F 64 bits
133
Encrypt
136
Block G 64 bits

FIG. 1

1/7

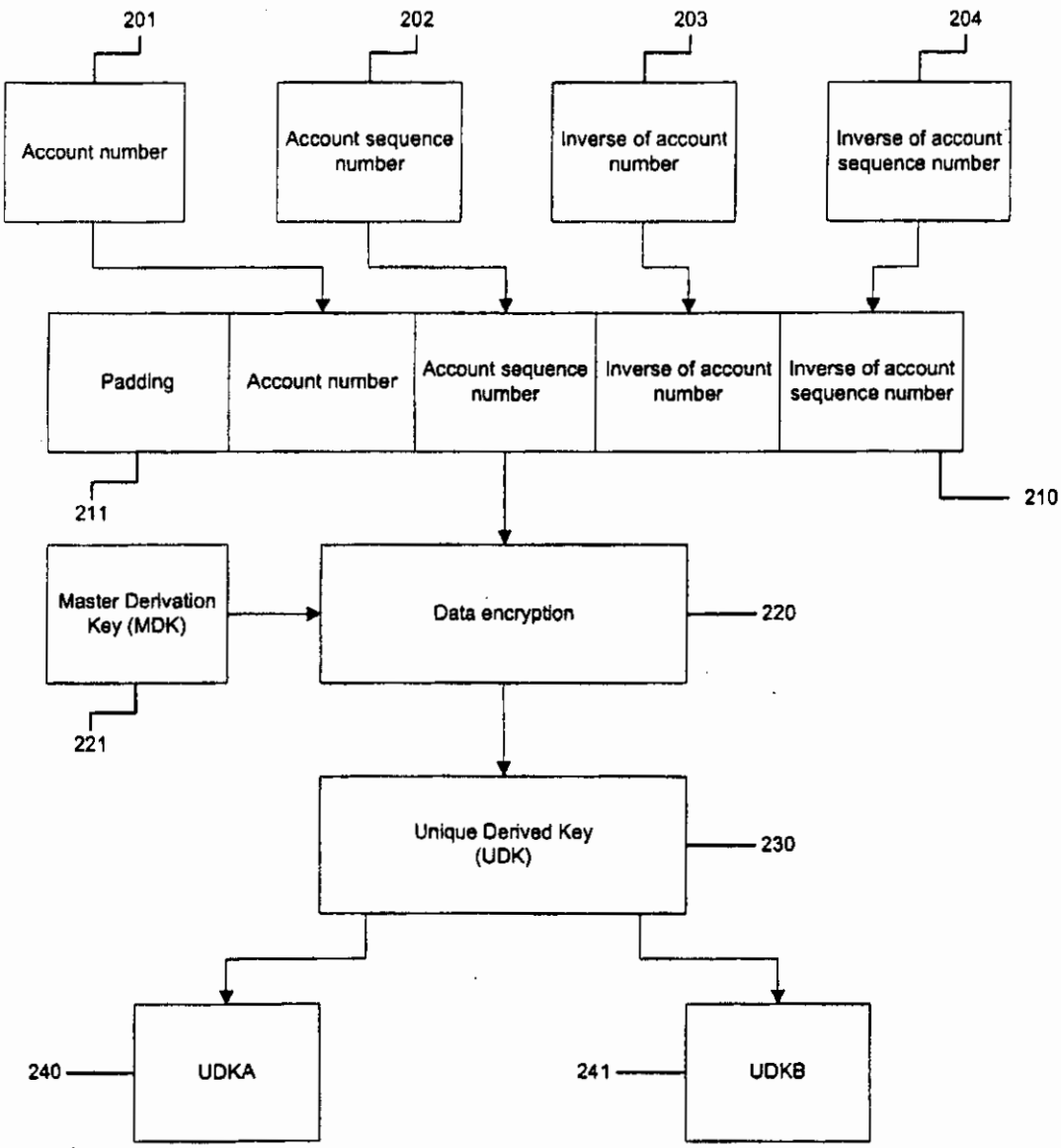

201
202
203
204
Account number
Account sequence number
Inverse of account number
Inverse of account sequence number
Padding
Account number
Account sequence number
Inverse of account number
Inverse of account sequence number
211
210
Master Derivation Key (MDK)
Data encryption
220
221
Unique Derived Key (UDK)
230
240
UDKA
241
UDKB

FIG. 2

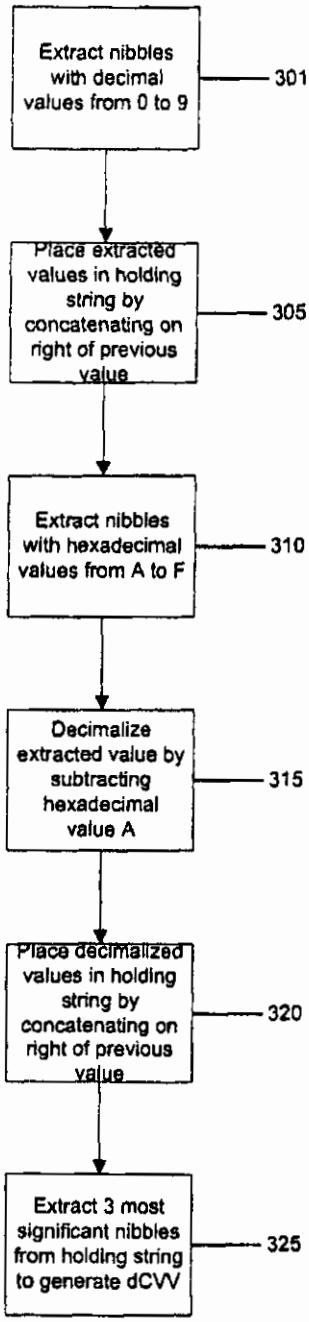

Extract nibbles with decimal values from 0 to 9
301
Place extracted values in holding string by concatenating on right of previous value
305
Extract nibbles with hexadecimal values from A to F
310
Decimalize extracted value by subtracting hexadecimal value A
315
Place decimalized values in holding string by concatenating on right of previous value
320
Extract 3 most significant nibbles from holding string to generate dCVV
325

FIG. 3

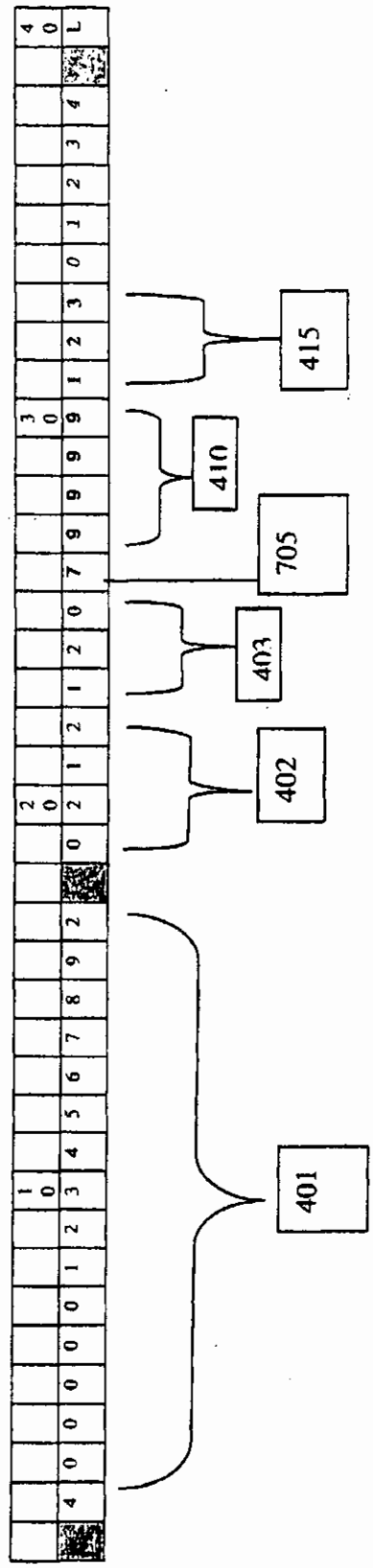


FIG. 4

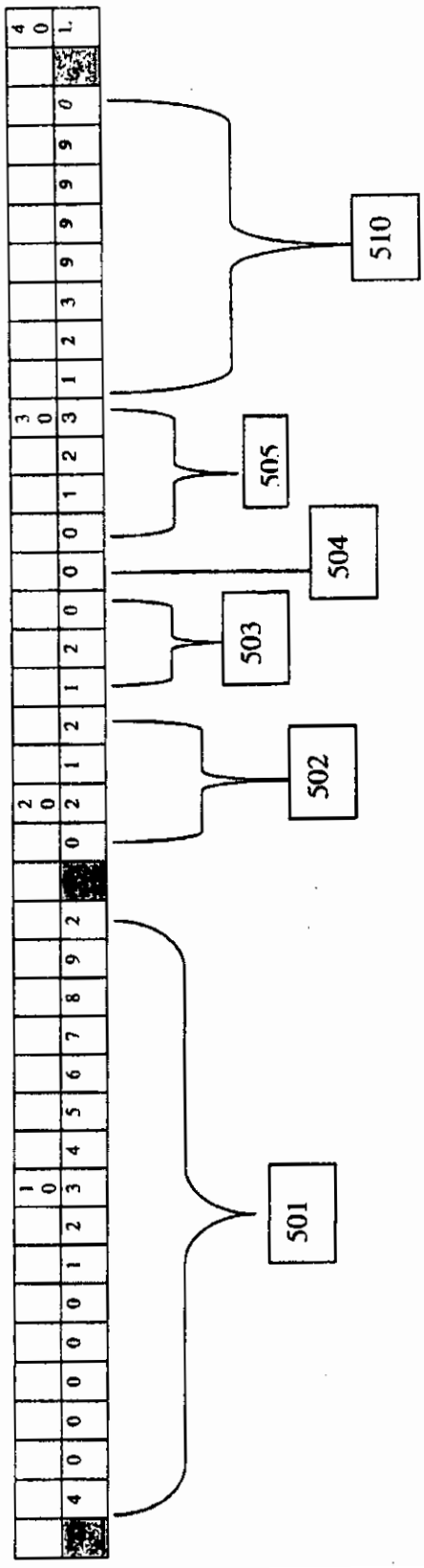


FIG. 5

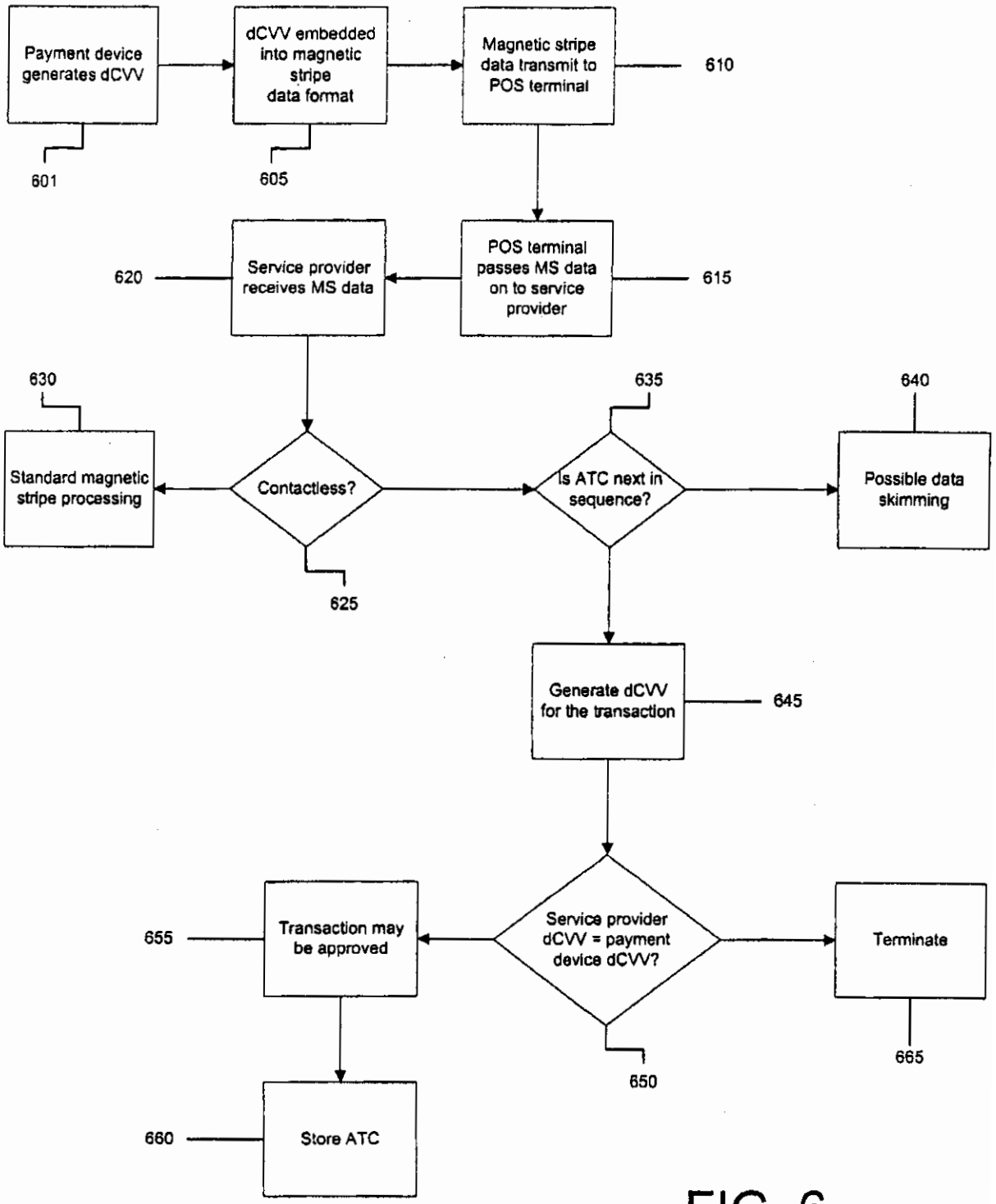

Payment device generates dCVV
601
dCVV embedded into magnetic stripe data format
605
Magnetic stripe data transmit to POS terminal
610
POS terminal passes MS data on to service provider
615
Service provider receives MS data
620
630
Standard magnetic stripe processing
Contactless?
625
635
Is ATC next in sequence?
640
Possible data skimming
Generate dCVV for the transaction
645
Service provider dCVV = payment device dCVV?
650
Transaction may be approved
655
Terminate
665
Store ATC
660

FIG. 6

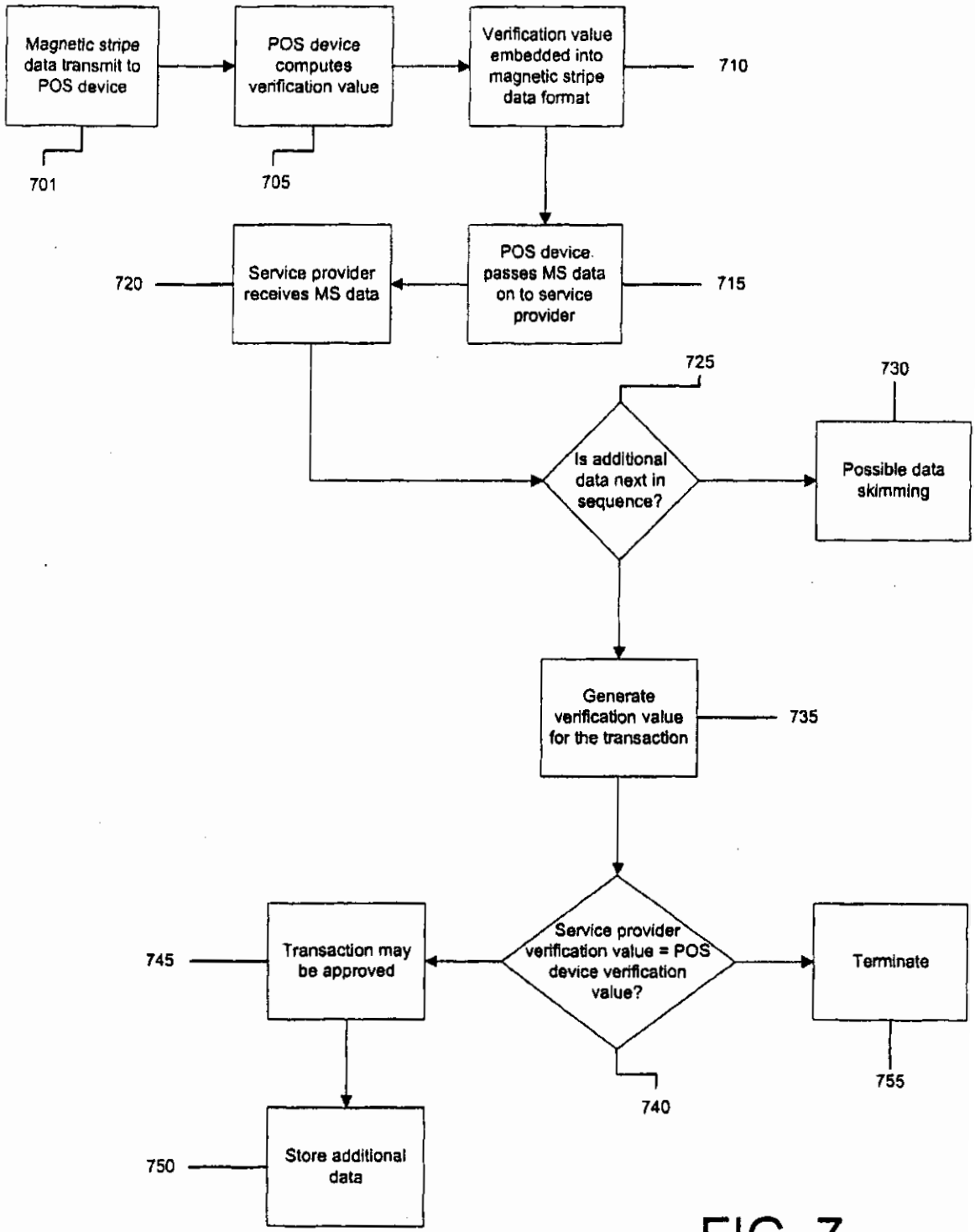

Magnetic stripe data transmit to POS device
701
POS device computes verification value
705
Verification value embedded into magnetic stripe data format
710
POS device passes MS data on to service provider
715
Service provider receives MS data
720
725
Is additional data next in sequence?
730
Possible data skimming
Generate verification value for the transaction
735
Service provider verification value = POS device verification value?
740
Transaction may be approved
745
Terminate
755
Store additional data
750

FIG. 7