

The Fiction of Secret POS Protocols – 101.x and 201.x

Forensic Analysis of a Persistent Payment Processing Scam

This white paper by International Finance Bank (IFB) dissects the pervasive myth of “secret POS protocols”

numbered from 101.1–101.9 and 201.1–201.9. Fraudsters claim these codes unlock privileged functions in payment terminals and card networks that bypass standard authorisation and settlement rules. In reality, no such protocols exist in Visa, Mastercard, American Express, UnionPay, EMVCo, or ISO 8583 specifications.

Each section provides:

- The Claim (fraudster's narrative)
- The Reality (how payments actually work)
- The Target Audience (who is lured in)
- Why It Works (psychology behind the scam)
- The Appeal (emotional hook used to close the sale)

101.1 – Instant Batch Override

The Claim: Hidden POS function to settle manually entered transactions instantly.

The Reality: All transactions require acquirer + issuer authorisation. Settlement is batch-based.

The Target Audience: Merchants under cash flow pressure; intermediaries seeking exclusive tools.

Why It Works: Exploits frustration over delays, ignorance of fixed clearing cycles.

The Appeal: Cash in your account instantly - no waiting.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -
> Acquirer -> Card Network -> Issuer
approval required

101.2 – Cross-Border Manual Settlement

The Claim: Force foreign cards to settle domestically for faster clearance.

The Reality: Routing fixed by network tables; terminals cannot alter.

The Target Audience: Merchants processing many international transactions.

Why It Works: Promises fee and time savings.

The Appeal: Treat any card like a local one - faster pay, lower cost.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

101.3 – Duplicate Card Data Injection

The Claim: Send identical transactions twice to trick system into approving.

The Reality: Networks detect duplicates; flagged as fraud.

The Target Audience: Intermediaries trying to recover failed sales.

Why It Works: Plays on gambler's fallacy.

The Appeal: Turn declines into approvals with a secret sequence.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

101.4 – Floor Limit Abuse

The Claim: Bypass issuer checks using floor limit loophole.

The Reality: Floor limits apply only to low-value contactless; manual entry always needs authorisation.

The Target Audience: High-value merchants wanting quick approvals.

Why It Works: Misuses legitimate industry term.

The Appeal: High-value transactions processed instantly - no oversight.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

101.5 – Merchant ID Override

The Claim: Switch to privileged merchant profile instantly.

The Reality: Merchant IDs fixed by acquirer; cannot be changed locally.

The Target Audience: High-risk MCC merchants.

Why It Works: Sells idea of 'clean' profile to bypass scrutiny.

The Appeal: Operate under a clean merchant profile at the touch of a button.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

101.6 – Card-Not-Present Forced Approval

The Claim: Convert online sales into card-present transactions for approval.

The Reality: CNP/CP coded in ISO 8583; mismatches declined.

The Target Audience: Online merchants with high declines.

Why It Works: Appeals to belief CP has fewer checks.

The Appeal: Make your online sales look like in-store swipes.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

101.7 – Manual Refund Exploit

The Claim: Refund without a sale to create credit.

The Reality: Refunds must match authorised transactions; unmatched credits blocked.

The Target Audience: Fraudsters seeking cash-out route.

Why It Works: Presents as exploiting refund systems.

The Appeal: Credit any account instantly - no sale needed.

Fake Flow

POS terminal sends 'protocol code' directly

Real POS Flow

POS terminal sends ISO 8583 auth request -

to network (no issuer check)

> Acquirer -> Card Network -> Issuer
approval required

101.8 – Manual Punching POS

The Claim: Manual key-in forces approval with backdoor merchant IDs.

The Reality: Manual entry still requires issuer authorisation; no bypass exists.

The Target Audience: Rejected high-risk merchants.

Why It Works: Appeals to those tired of declines.

The Appeal: Never get a decline again - every card works.

Fake Flow

POS terminal sends 'protocol code' directly
to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -
> Acquirer -> Card Network -> Issuer
approval required

101.9 – Blind Settlement Injection

The Claim: Inject settlement data directly, bypassing authorisation.

The Reality: Settlement files matched to auth logs; unmatched rejected.

The Target Audience: Payment newcomers unfamiliar with reconciliation.

Why It Works: Sells illusion of direct access to network.

The Appeal: Upload your own payments - no bank required.

Fake Flow

POS terminal sends 'protocol code' directly
to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -
> Acquirer -> Card Network -> Issuer
approval required

201.1 – Delayed Authorisation Sweep

The Claim: Batch transactions to avoid real-time checks.

The Reality: Still require issuer approval; funds not released without it.

The Target Audience: Low-connectivity merchants.

Why It Works: Abuses store-and-forward concept.

The Appeal: Approve sales even offline.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.2 – Cross-Acquirer Blind Push

The Claim: Route transactions to different acquirer on demand.

The Reality: Routing fixed by merchant-acquirer contract.

The Target Audience: Merchants wanting lower fees or less scrutiny.

Why It Works: Suggests secret processor choice.

The Appeal: Send your transactions to the bank you choose.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.3 – Offline POS

The Claim: Hidden mode processes offline transactions bypassing authorisation.

The Reality: Offline EMV still requires later issuer approval; TAC/IAC used, not 201.3.

The Target Audience: Remote-location merchants.

Why It Works: Uses real offline concept minus approvals.

The Appeal: Keep selling even cut off from the network.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.4 – Multi-Card Aggregation

The Claim: Combine small sales into large one to bypass limits.

The Reality: Violates rules; triggers fraud alerts.

The Target Audience: Small-ticket merchants wanting large-ticket capacity.

Why It Works: Sells blending into low-risk profile.

The Appeal: Hide large sales inside small-ticket processing.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.5 – Pre-Auth + Completion Ratio 1/10000

The Claim: One in 10,000 completions bypasses pre-authorisation.

The Reality: Every completion must match a pre-authorisation; no tolerance exists.

The Target Audience: Intermediaries chasing big single sales.

Why It Works: Uses pseudo-statistics for credibility.

The Appeal: Slip through a high-value sale - 1 in 10,000 odds.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.6 – Cascading Authorisation

The Claim: If declined, retry with another issuer.

The Reality: Only BIN-specific issuer can authorise.

The Target Audience: Merchants with high declines.

Why It Works: Sells 'second chance' approval.

The Appeal: Never stop at one decline - try again.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.7 – Stand-In Exploit

The Claim: Force STIP to approve large transactions.

The Reality: STIP capped low; high-value requires issuer input.

The Target Audience: Merchants wanting approvals during outages.

Why It Works: Misuses real fallback process.

The Appeal: Approve big sales even if bank offline.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.8 – Token Override

The Claim: Replace card data with trusted token.

The Reality: Tokens verified; mismatches declined.

The Target Audience: Fraudsters with invalid card data.

Why It Works: Uses security buzzword for credibility.

The Appeal: Use golden key token to unlock any payment.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

201.9 – Negative Settlement Offset

The Claim: Post negative to create credit with no debit.

The Reality: All clearing entries reconcile; unmatched rejected.

The Target Audience: Those seeking 'cash from thin air'.

Why It Works: Plays on accounting misconceptions.

The Appeal: Credit accounts from nothing with a negative post.

Fake Flow

POS terminal sends 'protocol code' directly to network (no issuer check)

Real POS Flow

POS terminal sends ISO 8583 auth request -> Acquirer -> Card Network -> Issuer approval required

Conclusion

These so-called POS protocols are fictitious. No official Visa, Mastercard, or EMVCo document contains them. They persist because they mix real industry terms with fabricated capabilities, fooling those with partial knowledge. At IFB Bank, we operate only within verifiable, regulated frameworks.