Virtual BIN: Preventive Recurring-Payment Control

Designing an Issuer-Controlled Virtual Payment Credential for Subscription Payments

Table of Contents

1. Data-Driven Problem Definition

- Subscription Growth and Loss of Consumer Control
- Dark Patterns and the Limits of Merchant-Controlled Cancellation
- Why Preventive Payment Control Is Needed

2. Three Core Functional Stages

- Stage 1. Subscription-Specific Virtual Payment Credential
- Stage 2. Rule-Based Authorization Control
- Stage 3. Credential Revocation and Future Authorization Blocking

3. Authorization Logic and Control Flow

- Consumer-Defined Rules
- Issuer-Side Authorization Checks
- Active Credential Management

4. Fraud Detection System (FDS) / Monitoring System

- Monitoring Repeated Billing Attempts
- Preventing Consumer Abuse of Disposable Credentials
- Active and Inactive Credential Separation

5. Quantitative and Qualitative Impact

- Consumer Protection
- Operational Benefits for Financial Institutions
- Market and Ecosystem Impact

Submitted to the 21st Financial Competition (FSS Korea). English translation for portfolio use.

1. Data-Driven Problem Definition

• Subscription Growth and Loss of Consumer Control

The digital subscription economy has grown quickly, and recurring payments are now part of everyday spending for many consumers. That convenience, however, also creates situations in which a payment relationship continues even after the consumer no longer wants it to.

Korea Consumer Agency data on online free-trial events found that, among categorized consumer-damage cases, insufficient notice of automatic conversion accounted for 34.0%, while restrictions on or obstruction of cancellation during the free-trial period accounted for 32.1%.[1]

A separate Korea Consumer Agency survey of 1,500 users of major OTT platforms found that 12.2% had experienced some form of dissatisfaction or consumer harm. Reported problems included excessive price increases, insufficient advance notice of changes, and refusal of subscription cancellation, early termination or refunds.[2] **These findings point to a structural imbalance: subscription enrolment can minimise friction while cancellation requires substantially greater effort.**

A consumer may be able to subscribe with one click or a stored credential, but leaving the service can involve several menus, confirmation screens or retention prompts. **This creates a gap between the consumer's intention to stop paying and the continued availability of a stored payment credential for future recurring charges.**

• Dark Patterns and the Limits of Merchant-Controlled Cancellation

One familiar example is the so-called "Roach Motel" design, where signing up is easy but leaving is not. Of course, a multi-step cancellation process is not automatically deceptive. Merchants may have valid reasons to confirm identity, explain what will happen after cancellation or prevent accidental termination.

The broader issue is that control over recurring payments often remains concentrated within the merchant's own interface.

Card issuers already evaluate fraud risk, available funds or credit, credential validity and other transaction conditions. Yet conventional authorization generally answers a different question: is this transaction technically valid and financially permissible? **It does not necessarily determine whether a recurring charge still reflects the cardholder's current payment preference.**

If a consumer wants to stop future charges, the normal route is still to return to the merchant's website or application. When that process is unclear, delayed or difficult, the stored credential may remain usable even though the consumer no longer intends to continue paying.

---

[1] *Korea Consumer Agency, "Online Events: Increasing Consumer Harm from Automatic Recurring-Payment Conversion after Free Trials," Consumer Damage Prevention Alert, Aug. 2025. Analysis of 151 consumer-redress applications received from 2022 through Q1 2025.*

[2] *Korea Consumer Agency, "Online Video Service (OTT) Satisfaction: High for Payment Convenience, Lower for Benefits," Service Quality Comparison, Aug. 14, 2025. Survey of 1,500 consumers.*

- Why Preventive Payment Control Is Needed

Refunds, disputes and chargebacks remain important consumer protections, but they are reactive by design. The payment has already been attempted or completed by the time the consumer contacts customer service or begins a dispute.

For a low-value recurring charge, the work required to recover the money can be disproportionate to the amount involved.

This project therefore moves part of recurring-payment control from post-transaction dispute resolution to pre-transaction authorization. Instead of relying only on the merchant's cancellation interface, a consumer could create and manage a subscription-specific payment credential through a banking or card application.

The scope is deliberately limited. Blocking a payment does not cancel the underlying service contract, and the consumer may still need to follow the merchant's formal cancellation process. **Its purpose is narrower: to give consumers direct control over whether a specific issuer-managed credential remains available for future recurring authorization attempts.**

2. Three Core Functional Stages

- Stage 1. Subscription-Specific Virtual Payment Credential

The first stage is to separate the subscription payment from the consumer's persistent underlying card credential.

When a consumer creates a credential for a subscription, the issuer would generate a Virtual PAN or Virtual Card Number linked securely to the underlying card or funding account. The merchant would receive the virtual credential rather than the primary card number.

In this project, "Virtual BIN" is used as the name of the proposed concept rather than as a claim that an individual consumer would literally receive a separate BIN. Technically, the consumer-facing instrument would be a Virtual PAN, Virtual Card Number or equivalent virtual payment credential. A dedicated virtual-card BIN or account range could be used as one implementation option to distinguish the relevant product environment, but such a structure would not be essential to the underlying control model.

The important part is not simply the existence of a second card number. It is the policy attached to that credential. The issuer could associate it with a permitted merchant, a maximum transaction amount, an expected billing frequency or transaction velocity, a validity period and a lifecycle status.

For example, a consumer might create a credential for one subscription provider with a KRW 15,000 spending limit, an expected monthly billing cycle and a 30-day validity period.

The innovation is therefore not the invention of virtual cards themselves, but the use of a purpose-specific virtual credential as a consumer-controlled authorization layer for recurring payments.

- Stage 2. Rule-Based Authorization Control

Once the merchant submits an authorization request, the issuer identifies the virtual credential and retrieves the policy attached to it. **The transaction is then evaluated against the consumer-defined merchant, amount, frequency or velocity, validity and credential-status conditions before normal authorization is completed.**

Merchant identification is one of the more difficult parts of the design. A subscription provider may use several Merchant IDs, regional entities, payment processors or payment facilitators. In practice, the system would need some form of normalized merchant mapping rather than a simple text comparison.

Available identifiers, merchant-group relationships and supporting information such as Merchant Category Codes could all contribute to that mapping. MCC alone would not be enough, since unrelated businesses can share the same category.

Billing frequency creates a similar problem. A rule such as “one payment per calendar month” sounds simple, but legitimate billing dates can move because of weekends, retries or processing variation. **A more realistic model would combine authorization count, transaction velocity, expected billing interval and timing tolerance.**

Where available, recurring-payment or stored-credential indicators carried in payment-network transaction data could also provide supporting metadata when recurring authorization requests are evaluated.[3]

Consider a credential intended for a monthly subscription of up to KRW 15,000. A KRW 14,900 charge from the recognized merchant within the expected billing window could proceed normally. A materially higher amount, an unrelated merchant or several unexpected attempts in a short period could instead lead to a decline or additional verification.

The result is a credential that carries its own payment rules, rather than simply another number linked to the same account.

- Stage 3. Credential Revocation and Future Authorization Blocking

The third stage gives the consumer a way to revoke or lock the subscription-specific credential from the banking or card application.

Once that credential is marked as revoked, later authorization attempts using it can be declined by the issuer.

Revoking the payment credential does not itself terminate the underlying subscription contract; it controls payment authority rather than the legal existence of the service relationship. A merchant may still require formal cancellation, and contractual obligations may remain.

The lifecycle issue matters here. Modern payment systems can use card-account updates, token updates or re-provisioning processes to maintain legitimate payment continuity when credentials change.

---

[3] Visa, Visa Core Rules and Visa Product and Service Rules, Apr. 2026, Table 5-22, “Processing Requirements for Transactions Using Stored Credentials.”

That is useful in normal circumstances, but it also means that an explicit revocation instruction has to survive later credential changes. **If the consumer explicitly revokes a subscription-specific credential, later credential updates or re-provisioning should not unintentionally restore that merchant's payment authority.**

For that reason, the revocation state should remain authoritative throughout the credential lifecycle.

3. Authorization Logic and Control Flow

- Consumer-Defined Rules

From the consumer's perspective, the control model can be reduced to four main variables: merchant, amount, frequency or velocity, and validity.

Those settings define the scope of permission granted to the merchant through the virtual credential.

Behind the interface, the issuer could maintain more detailed information, including the linked funding account, normalized merchant mapping, transaction-count rules, billing-window tolerance and lifecycle status.

Instead of treating a stored credential as indefinitely reusable, the model turns payment authority into a defined and revocable set of permissions.

- Issuer-Side Authorization Checks

When an authorization request arrives, the issuer retrieves the policy attached to that credential and compares the transaction with its restrictions. Existing controls for fraud, available funds or credit and other transaction risks would continue to run alongside the subscription-specific rules.

If the conditions are satisfied, the transaction proceeds through normal authorization; if a condition is violated, the issuer may decline the transaction or require additional consumer verification.

In practice, not every mismatch should produce the same response.

A modest subscription price increase, for example, may justify asking the consumer for confirmation rather than rejecting the merchant permanently. A retry after a temporary failure can be assessed in the context of the earlier attempt. Use of a merchant-specific credential by an unrelated merchant is much clearer and could be declined immediately.

The objective is not a simplistic allow-or-block filter, but a system that translates explicit consumer preferences into enforceable issuer-side authorization rules.

- Active Credential Management

Real-time authorization also requires the relevant control data to be easy to retrieve.

An issuer could maintain a dedicated set of active credential records containing the credential identifier, linked account, permitted merchant information, amount limit, billing rule, validity period and lifecycle status.

Historical transaction information could still be referenced when needed for velocity or risk analysis. The current authorization state, however, should remain directly accessible.

The proposal therefore adds a subscription-specific control layer to existing issuer authorization infrastructure rather than requiring a new card network.

No specific processing-time claim is made here. Actual latency and performance would need to be tested through implementation and benchmarking.

4. Fraud Detection System (FDS) & Transaction Monitoring

- Monitoring Repeated Billing Attempts

The proposed control layer would sit alongside existing fraud-detection and transaction-monitoring systems.

A revoked or restricted credential may still receive authorization attempts, but repeated attempts should not automatically be treated as misconduct. Merchants may retry charges because of insufficient funds, temporary processing failures or ordinary retry logic.

Context therefore matters.

Transaction velocity, Merchant IDs, merchant-group relationships, MCCs, amounts, timing, credential status and similarity to earlier attempts could all be used as signals. One retry after a temporary failure may be normal. Repeated requests against a credential the consumer has explicitly revoked would be more significant.

The issuer cannot necessarily stop the merchant or acquirer from sending an authorization request, but it can control how that request is handled once it reaches the issuer environment.

Depending on issuer policy, a request against a revoked or non-compliant credential could be declined automatically, monitored more closely or routed for further investigation.

- Preventing Consumer Abuse of Disposable Credentials

The control mechanism also introduces a risk on the consumer side.

A customer could repeatedly generate short-lived credentials, for example, in an attempt to obtain multiple free trials from the same provider.

The issuer would therefore need to preserve the link between individual virtual credentials and the underlying customer or funding account. Issuance controls could take into account the number of recently created credentials, merchant group, credential type, transaction history and customer behavior.

Consumer control should be strengthened without creating an unrestricted way to bypass legitimate merchant policies or repeatedly exploit promotional offers.

- Active and Inactive Credential Separation

Active and inactive credentials should also be treated differently.

Active credentials need to be available quickly because legitimate authorization requests may still arrive. Revoked or expired credentials no longer need the same real-time access, but they can still be relevant for audit, dispute investigation, lifecycle enforcement and monitoring.

Keeping these states separate can simplify the real-time authorization path while preserving historical information needed for control and investigation.

The exact storage design would depend on the issuer's own infrastructure and implementation requirements.

5. Quantitative and Qualitative Impact

- Consumer Protection

The original analysis included an illustrative scenario using approximately 28 million card users, an assumed 5% incidence of one unwanted annual renewal and an average unwanted payment of KRW 15,000.

Under those assumptions, the total would be approximately KRW 21 billion.

The KRW 21 billion figure is an illustrative sensitivity scenario, not an observed estimate of actual market-wide losses. The population base and 5% incidence are scenario inputs rather than estimates of the actual number of consumers experiencing unwanted renewals.

The point of the calculation is simply to show that small recurring charges can become economically meaningful when considered across a large customer base.

The direct consumer benefit is an additional control point before an unwanted recurring charge becomes a dispute that must be resolved after the fact.

- Operational Benefits for Financial Institutions

Recurring-payment problems can generate customer-service enquiries, transaction investigations, merchant communication and, in some cases, formal disputes or chargebacks.

If some unwanted transactions can be stopped before successful authorization, at least part of that downstream workload could be avoided.

The model shifts part of the operating process from reactive dispute handling toward preventive authorization management.

It could also make the issuer's banking or card application more useful for day-to-day payment management by allowing subscription-specific credentials, limits and revocation decisions to be handled in one place.

Any effect on engagement, satisfaction, retention or cross-selling would still need to be demonstrated with actual implementation data.

The technical building blocks themselves do not require an entirely new payment infrastructure. Virtual card numbers linked to funding accounts, amount and validity controls, merchant restrictions, transaction or velocity controls, issuer authorization and credential lifecycle management are all conceptually compatible with modern payment systems.

The proposal's principal innovation is the integration of these capabilities into a consumer-facing control model specifically designed for recurring subscriptions.

A production implementation would still need to validate merchant identification, billing tolerance, network rules, credential-update behavior, retry handling, legal requirements and issuer-specific infrastructure.

- Market and Ecosystem Impact

At the market level, the proposal changes where recurring-payment control can be exercised.

The merchant remains responsible for the underlying service relationship, contractual terms and formal cancellation process. The consumer, however, gains direct control over whether an issuer-managed credential remains available for future payment attempts.

Service cancellation and payment credential authority are related, but they are not technically or legally the same decision. The model deliberately keeps that distinction intact.

An additional issuer-side control layer could also reduce the extent to which subscription retention depends only on friction within the merchant's cancellation interface. Over time, that may encourage providers to compete more strongly through service quality and customer value rather than barriers to exit.

By combining purpose-specific virtual payment credentials, consumer-defined authorization rules, issuer-side checks, lifecycle revocation and transaction monitoring, the model shifts recurring-payment protection from a predominantly reactive process toward a more preventive one.

Its central proposition is simple: **a recurring payment should remain authorized only while the consumer-defined payment authority attached to that credential remains valid.**