Dyno Systems
DYNAMIC CARD SOLUTIONS

Abstract

Payment card fraud remains a multi-billion-dollar threat to banks and consumers. **Dyno Systems** addresses this by eliminating static Primary Account Numbers (PANs) on cards and using dynamic tokenization. Each transaction uses a one-time token or changing PAN and CVV, typically managed via a secure app. No card number or CVV is printed on the card itself, preventing skimming or data theft from physical or online use. This paper explains Dyno's method of **rotating card data** and compares it with conventional Visa/Mastercard cards and virtual/fintech alternatives. We show how Dyno's approach (akin to network tokens and dynamic CVV) can slash fraud rates by up to ~60% usa.visa.com, accelerate card reissuance, and save banks and consumers millions in losses and logistical costs. Quantitative estimates and illustrative charts highlight potential savings in fraud losses and replacement costs under Dyno's model.

Introduction

Payment card fraud is surging as more transactions move online. Global card fraud losses reached ~$33.8 billion in 2023 globenewswire.com, and are projected to hit ~$404 billion over the next decade globenewswire.com. In the U.S. alone, card-not-present (CNP) transactions (e-commerce, mail/phone order, etc.) now drive the bulk of fraud losses globenewswire.com, since stolen static card data can be reused indefinitely online. Notably, studies estimate 46% of fraud occurs in the U.S. and that **up to 80% of issued cards have already been compromised** via breaches merchant cost consulting.commerchantcost consulting.com. Each stolen card number forces issuers to cancel and reissue cards – a costly process (often $5–$20 per card econinfosec.org) that frustrates customers. Banks also absorb chargebacks, investigations, and reputational damage (every $1 of fraud costs banks ~$3–$4 in indirect losses businessinsider.com globenewswire.com). Against this backdrop, Dyno Systems' dynamic card aims to *prevent* most card-fraud by design, offering banks and users greater security and lower operational expense.

Technology Overview of Dyno Systems

Dyno's **dynamic card** eschews any permanently printed PAN, CVV or expiry date. Instead, the card holds only minimal information (e.g. owner name or even just a reference). All sensitive data is stored in the issuer's secure token vault or user's mobile app. When a customer makes a purchase, the system generates a **unique dynamic token or number** for that transaction (or rotates the card's EMV PAN/CVV on a schedule). In practice this uses standard payment tokenization frameworks: the static PAN is replaced by a cryptographic token tied to the merchant and device. For example, Visa and Mastercard network tokens already work this way for digital wallets usa.visa.com pymnts.com. Dyno extends this to the physical card: an e-ink display or mobile app updates the CVV (and potentially the PAN) each hour or transaction. After one use or time interval, that token expires and cannot be reused.

Key features of Dyno's design include:

- **Dynamic Tokenization** – Each transaction uses a one-time PAN-like token (or dynamic CVV) instead of the original account number. The real MAN never leaves the secure vault usa.visa.com.

- **Rotating Numbers** – The card's displayed number (and/or CVV) refreshes regularly, so stolen data quickly becomes useless businessinsider.com link-info.com. For example, Idemia's "Motion Code" card used an E-Ink display to change the CVV hourly, making fraud from static CVVs impossible-ink-info.come-ink-info.com. Dyno applies the same principle to the entire card number.

- **Numberless Card Surface** – Similar to Apple Card and iFAST bank's offerings, Dyno prints no PAN, CVV or expiry on the plastic fastcompany.com financialit.net. A user receives their account details securely in an app or via contactless activation. This eliminates risks from skimming or photos of the card; all merchants must either use the chip (EMV) or read a temporary number from the app.

Together, these innovations form a *multi-layered security model*. Even if a criminal obtains the card or intercepts a number, by the time they attempt to use it the data has changed. Moreover, Dyno can incorporate additional authentication (biometrics or device verification) via the app, making the physical card alone insufficient for fraud. This self-evolving token scheme (as described in recent research on dynamic tokenization researchgate.net) greatly hardens the payment system against modern attacks.

Market Comparison

Traditional Card Networks (Visa/Mastercard)

Legacy credit/debit cards have **static PANs** embossed or printed on them, and a fixed CVV. While EMV chips and contactless tokens have improved security in person, online fraud remains vulnerable. Visa/Mastercard are moving toward tokenization. Their network tokens replace the PAN in digital wallets and can be updated if a card is reissued. In fact, Visa reports network tokens now enable 29% of transactions and have **saved $650 million in fraud last year**, roughly a 60% reduction in fraud ratesusa.visa.com usa.visa.com. However, this mostly protects *e-commerce*, not the physical card. The static print on a plastic card (and its CVV) remains a single point of failure: criminals who steal or copy this can transact anywhere not using dynamic verification.

Some traditional banks have piloted dynamic solutions. For instance, Thales/Gemalto's **Dynamic Code Verification (DCV)** card shows an E-Ink CVV on the back that changes every hour cpl.thalesgroup.com link-info.com. PNC tested Idemia's Motion Code, and it cuts online fraud by forcing criminals to have the card present at the exact minute e-ink-info.com. But with traditional issuers this typically requires customized expensive cards (Idemia estimated ~$15 each e-ink-info.com, vs $2–$4 normally). Banks also still issue static-PAN cards by default, so a stolen photo or skimmer copy still works until the CVV cycles.

Virtual Cards and Fintech Solutions

Modern fintech and digital wallets increasingly remove static data:

- **Apple Card (Titanium)** – Apple's physical card *only* shows the cardholder's name fastcompany.com. The virtual number and security code live in the Wallet app, where the user can generate a new CVV on demand. If the physical card is inspected or skimmed, no useful number is exposed. This mirrors Dyno's "card-less" design.

- **Virtual/Disposable Cards (Privacy.com, Revolut, etc.)** – Services like Privacy.com let users create one-time virtual card numbers per merchant. These random PANs can be locked or revoked instantly if compromised. In effect, each vendor gets a **unique token** instead of the real account. Similarly, many neobanks (Revolut, Monzo) and even Amex/Citi offer **per-merchant virtual account numbers** or CVVs for online use. Such cards minimize fallout from breaches: even if a token leaks, it can be disabled without touching the main account. Dyno offers the same

tokenization but bound to a secure physical card, covering both online and in-person use.

- **Other Fintech Cards** – Some new cards adopt dynamic CVVs (e.g. Brex Card's in-app CVV for online payments) or integrate biometric unlocking. As one study notes, combining tokenization with FIDO2/biometric authentication further "addresses the human element in security" researchgate.net. Dyno's app could likewise require user fingerprint before revealing a new PAN, adding another layer.

In summary, **Dyno surpasses legacy static cards** and matches or extends cutting-edge fintech: it couples Visa/Mastercard tokenization benefits usa.visa.compymnts.com with the no-PAN design of virtual cards fastcompany.com financialit.net, but in a single physical card. This unity offers seamless use in any terminal (chip, magstripe or online) without exposing long-lived credentials.

Fraud Prevention Efficacy

By continuously changing card details, Dyno essentially neutralizes many common fraud methods. A static card number can be phished, skimmed, or stolen and then misused repeatedly. In contrast, every stolen Dyno token expires quickly. Visa's data suggests tokenization **cuts fraud by up to 60%** usa.visa.com. Mastercard similarly reports that migrating to tokenized credentials **reduces fraud and boosts approval rates by 3–6 percentage points** pymnts.com. In practice, if a hacker obtained today's PAN from a Dyno card, it would already be obsolete by the next hour. Even if a purchase goes through, the bank instantly replaces the token; subsequent unauthorized attempts fail.

Empirical evidence underscores these gains. The Nilson Report notes U.S. fraud is heavily CNP-driven globenewswire.com. Removing static numbers eliminates almost all CNP misuse: without a fixed CVV or PAN, online-only thieves have nothing to use. For card-present fraud (skimming, cloned chips), Dyno's chip can still be used, but digital blocklists and token revocation can stop a stolen card from working after one use. Overall, Dyno's multi-factor, rotating token approach creates layers of defense. One industry survey emphasizes that multi-layered measures (behavioral analysis, tokens, biometrics) yield much lower fraud costs risk.lexisnexis.com. Dyno contributes powerful layers by design.

Faster, Cheaper Reissuance

Traditional card replacement is slow and costly. Each new plastic requires production, personalization and mailing; issuers typically spend $3–$25 per reissued card econinfosec.org. After a data breach or loss, banks scramble millions of cards. For example, following large breaches, some banks reported costs of $5–$6 per card reissue decon infosec.org. These costs are largely logistical and fixed. Dyno dramatically reduces this burden. Because Dyno cards have no fixed number or CVV printed, most fraud or loss incidents can be handled digitally: the bank simply invalidates the old token and reissues a new dynamic identity via the app. The physical card can be reactivated remotely or replaced on an extended cycle since it contains no sensitive data. This means **fewer emergency mailings**. Even if a card is physically lost, the "reissuance" becomes mostly a PIN change in the app, not a five-dollar plastic order. For large issuers with millions of cards, this represents millions of dollars saved per year in production and postage.

Cost Savings and Benefits (Illustration)

Consider a hypothetical portfolio of 100,000 active cards. Typical U.S. card fraud runs around **0.1–0.2%** of volume. If annual volume is $100M, fraud losses might be $100–200K. With Dynos ~60% reduction usa.visa.com, fraud could drop to $40–80K, saving $60–120K (excluding the 3–4× multiplier on indirect costs risk.lexisnexis.com). Simultaneously, if 1% of customers normally require a new card each year due to loss/breach (1,000 cards), at $10 each that's $10K in printing/ship. Dyno could halve that by using digital replacements. The net effect: **banks save tens of thousands per 100k cards**. In graphical terms, a bar chart (Figure 1) would show fraud costs and issuance costs slashed under Dyno versus static.

For consumers, the benefits are easier life and more confidence. They face fewer fraudulent charges and less hassle disputing them. They avoid the weeks-long inconvenience of waiting for a new card. With Dyno, an online profile breach is largely moot, since a user's apps simply generate new tokens. Customer surveys confirm security drives satisfaction: e.g., 83% prioritize security in payments pymnts.com, and tokenization's "peace of mind" is a key selling point usa.visa.com usa.visa.com.

(Figure 1: Estimated annual costs per 100k cards under static vs Dyno system. Bars denote fraud losses and card issuance costs; Dyno drastically reduces both.)

Conclusion

Dynamic tokenization, rotating PAN/CVV and numberless cards represent the next leap in payment security. Dyno Systems combines these into one solution. By removing static

card credentials and automating fresh tokens each time, Dyno can cut fraud rates by a majority of usa.visa.com, eliminate vast swaths of CNP fraud globenewswire.com, and slash card replacement overhead. Visa's experience shows tokenized credentials both save hundreds of millions in fraud and raise authorization rates usa.visa.com pymnts.com. For banks, this means lower losses, lower compliance costs, and more customer trust. For consumers, it means faster recovery from theft and year-round peace of mind. Our analysis (supported by industry data businessinsider.com globenewswire.comecon infosec.org) suggests Dyno's dynamic card could deliver *order-of-magnitude* savings in fraud-related costs while enhancing user experience. As payment ecosystems evolve, such self-resetting card systems seem poised to become the new standard for safety and efficiency.