KEYNO

The Standard for
Online Fraud Prevention

THE ONLINE FRAUD CHALLENGE:

How Dynamic Security Codes Safeguard Payments

Dynamic security codes, or dCVV2, take fraud prevention to the next level. By replacing static codes with randomly generated versions that change regularly, dCVV2 safeguards the card *and* the cardholder—and complements existing fraud prevention solutions. Here's everything issuers need to know about dCVV2, including how it's easily enabled—requiring no tech development—and keeps cards top-of-wallet.

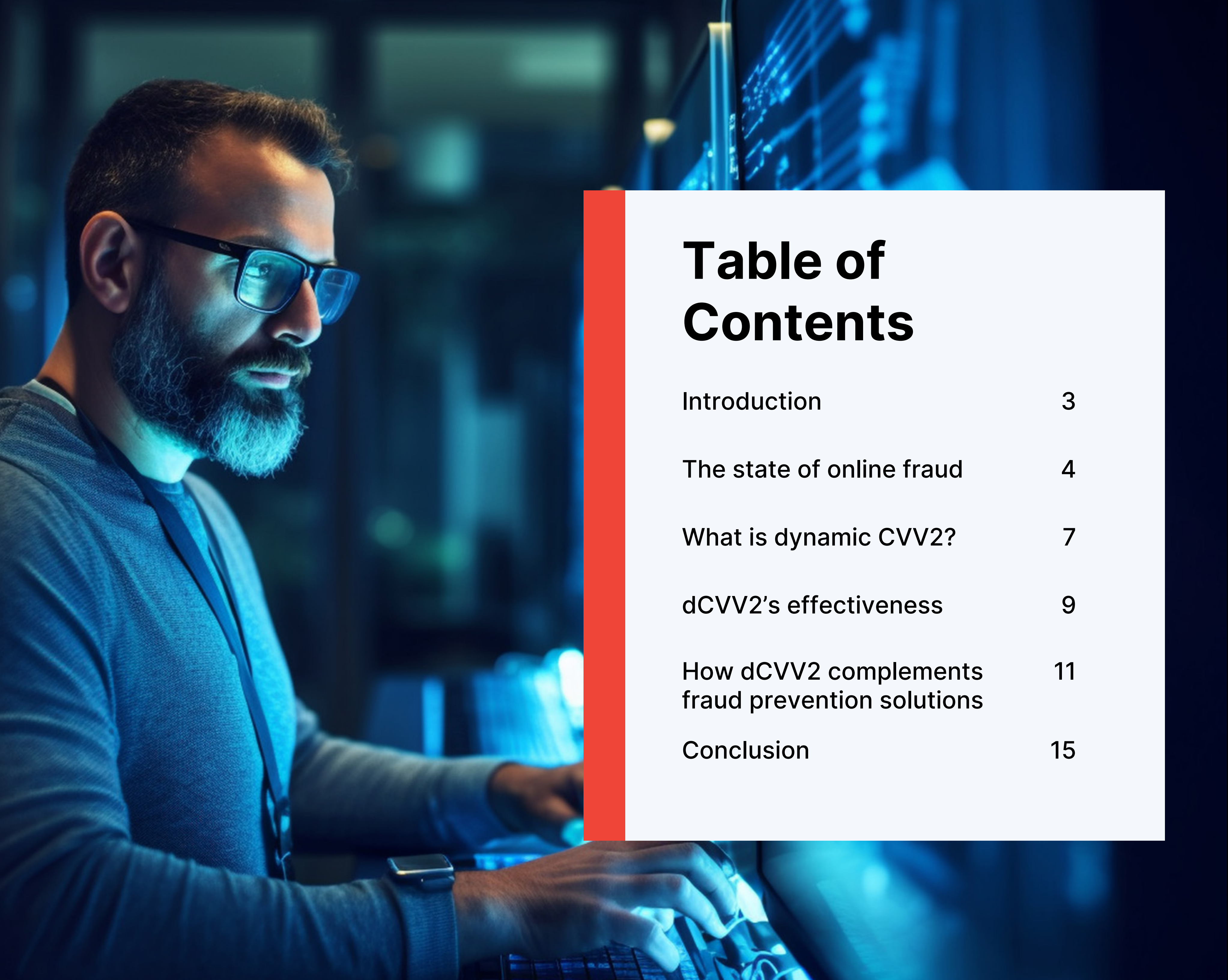


Table of Contents

Introduction

It’s no secret that fraud is rising faster than ever and getting more costly.

What is surprising is the alarming increase in online fraud. Card not present (CNP) payment transactions and e-commerce have become ground zero for card fraud.

Static card verification value (CVV) security codes are remarkably vulnerable—and shockingly easy to crack: sophisticated hacking operations can turn up matches in as little as six seconds. The rise of generative AI and the potential of deepfakes only add to the threats.

Dynamic CVV2 (dCVV2) technology eliminates those vulnerabilities. The always-changing security codes are a tailor-made solution to a sobering reality in today’s CNP fraud environment: card thieves are intent on shopping, not merely creating counterfeit plastic cards. As a result, the card industry is racking up staggeringly large financial losses.

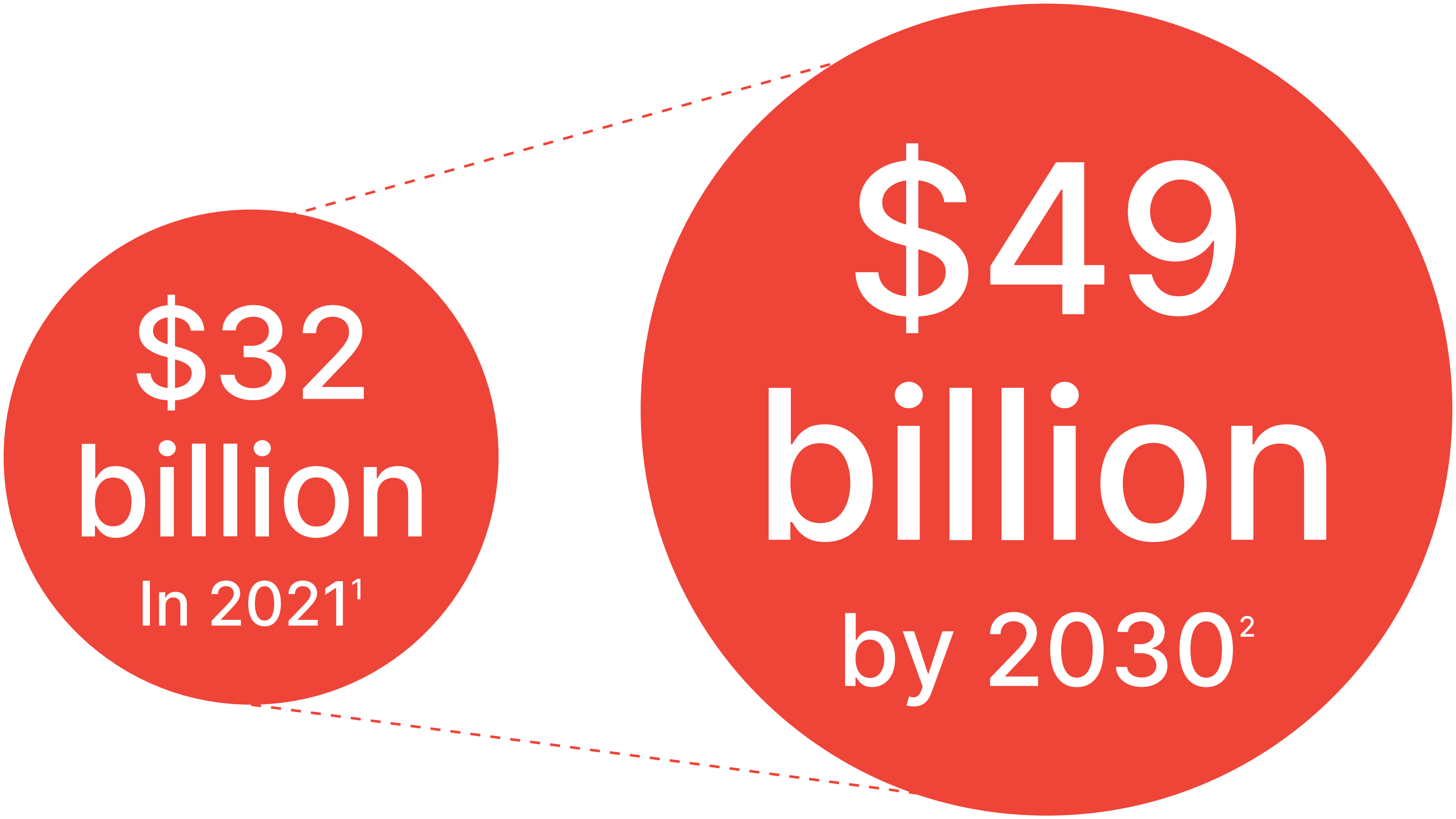
Yet dCVV2 technology maintains a relatively low profile among card issuers.

How Dynamic Security Codes Safeguard Payments examines the technology and how it works. We explore not only how dynamic security codes tackle the vulnerabilities of the digital environment but also how they enhance fraud protection portfolios—complementing tokenization, 3DS, and AI/ML—and help lower card issuers’ fraud-related business costs such as replacement cards, reduced card usage, customer attrition, and fraud losses.

Here’s everything you need to know about how dCVV2 can provide CNP fraud prevention to keep your card top-of-wallet.

The state of online fraud

Annual global card fraud losses are soaring.



$32 billion

In 2021[1]

$49 billion

by 2030[2]

Card fraud is growing more sophisticated.

Organized threats are rising . . .

Global digital transactions skyrocketed to 39.4 billion within six months, an astonishing 37% increase in volume YOY—matched by a 38% increase in automated bot attacks.[3]

. . . as fraud becomes more lucrative,

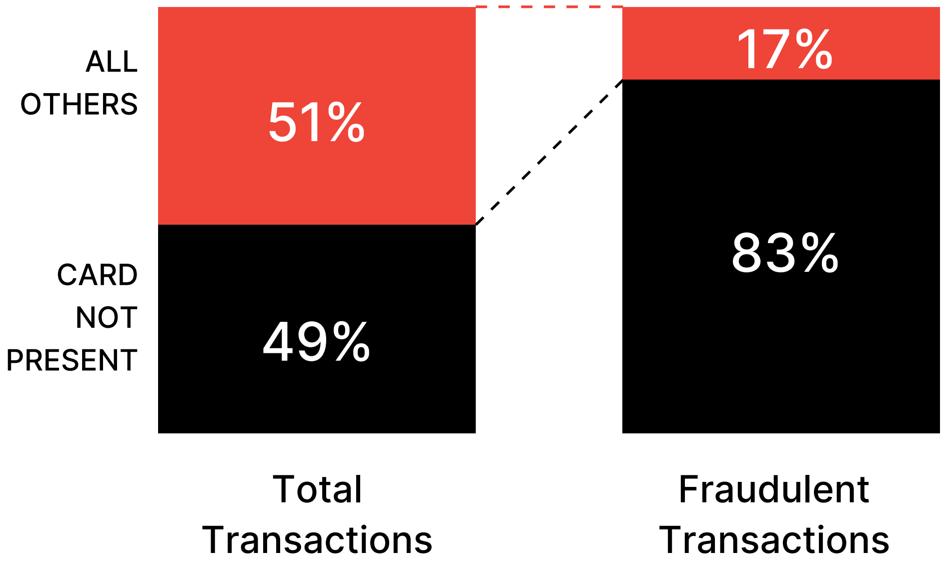
Card fraud netted criminals nearly $4 billion more in 2021 than in 2020. Criminals saw a 14% growth in the money they were able to steal from the system.[4]

. . . and the dark web marketplace explodes

45.6 million CNP payment cards were posted for sale on the dark web in 2022.[5]

The majority of fraud occurs online—and is costly for banks

Online transactions make up less than half of total purchases yet account for more than 4 in 5 cases of payment card fraud.



Source: TK

$4.23

In the U.S., each dollar lost to fraud attacks in 2021 cost U.S. banks and financial services firms $4.23, up more than 16% from 2020.

What is dynamic CVV2?

Digital technology renders static CVV codes obsolete.

When EMV chip technology brought enhanced security to card-based transactions, fraudsters shifted their focus to CNP transactions.

CVV codes were a pre-emptive strike against CNP fraud. Together with the primary account number (PAN) and expiration date, the security codes provided a much-needed second level of authentication for online purchases. Because the Payment Card Industry (PCI) standards prohibit merchants from storing the codes, consumers' card data gained an added line of defense against hackers and breaches.

But CVVs also opened gaps in fraud protection. For one thing, the codes are static. They're a fixed data point that, like PANs and PII data, is vulnerable to theft. For another, once merchants place the card's data on file after an initial transaction, many will process subsequent transactions without requesting the CVV code.

Perhaps most alarming, guessing CVVs is surprisingly easy. Sophisticated hacking operations that deploy web bots to wage enumeration attacks can turn up code matches in as little as six seconds, according to researchers at Newcastle University in the UK.

Enter dynamic CVV2

dCVV2 eliminates those vulnerabilities. Using digital technology, it generates new CVV codes at set time intervals so that even if the code is hacked, it's viable only for a short time. Stolen credentials quickly become obsolete. Reusing the code is nearly impossible.

In its earliest form, dCVV2 was embedded in physical cards that displayed the code on a small LCD. But the cards are expensive to produce, costing issuers $12 to $15, or eight to 10 times as much as cards with EMV chip technology.

A more natural, targeted, and cost-effective delivery of dCVV2 technology is through mobile apps and browser-based solutions. To initiate a payment transaction, customers request the security code from the authenticator app or banking app on a mobile device, or through the browser. The card network checks the code during authorization, and then forwards the pass/fail result to the issuer or responds to the acquirer on the issuer's behalf. The code expires within a set interval of time. For merchants, dCVV2 requires no additional work—no changes in process, and no investment in technology or infrastructure.

Fraud protection where payments are made

Equally important, delivery of dCVV2 through mobile applications and browser extensions targets CNP fraud where it's happening.

An astonishing 91% of Americans ages 18 to 49 use their smartphone to make online purchases, according to a 2022 report by the Pew Research Center. And it's not just younger consumers: Gen X and Baby Boomers are also tech-savvy, with 69% of those 50 to 64 using their smartphone to buy online, and 48% of those 65 and older.

Receiving security codes via smartphone is the natural accompaniment to paying by smartphone.

dCVV2's effectiveness

Dynamic security codes provides card issuers with a host of benefits.

Eliminates fraud. A 2022 Visa case study on dCVV2 showed a CNP fraud reduction of 91.3% on a credit card portfolio and a similar 70.8% CNP fraud reduction on a debit card portfolio. Since the original study, five other banks have reported CNP fraud reductions of over 95%. Dynamic CVV2 works because the code is always checked at the network level regardless of transaction size and a dynamically changing CVV2 code makes compromised card details obsolete before they can be used. dCVV2 also enables authentication that safeguards against enumeration attacks—a critical factor in the US, which is the most heavily targeted geography for programmatic testing attacks, on both the acquiring side (63.5% of total acquiring enumeration) and issuing side (38.8% of total issuer enumeration). In addition, banks that have implemented dCVV2 have seen an increase in merchant credits related to friendly fraud. The dCVV2 security code is traceable to a specific cardholder action and window of time, so it's harder for cardholders to dispute the transactions. Friendly fraud is costly for merchants—and growing costlier. In a recent survey, merchants reported a 19% increase in illegitimate chargebacks in early 2023 over the same period in 2022.

dCVV2 protects across all online transactions

CUSTOMER 1: MID-SIZE US BANK

12-month pilot with 1,000 cards

CNP Credit Card Fraud in Last 12 Months

Basis Points

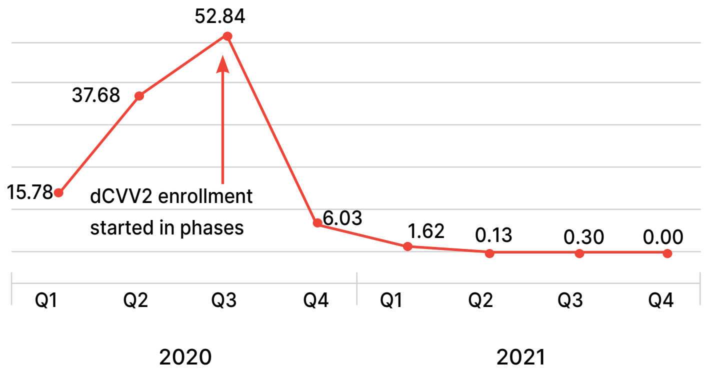
0 bps	22.83 bps
With dCVV2	Without dCVV2

CUSTOMER 2: LAC BANK

All cards enrolled in dCVV2

CNP Credit Card Fraud by Quarter

Basis Points



Source: Visa. dCVV2 solution provided by KEYNo.

Increased approval rate. Dynamic CVV2 security codes eliminate 85% of false positives, which are legitimate transactions flagged as fraudulent. The additional data point enables the system to become more confident and as a result alter the risk score. The increased approvals dramatically reduce a major point of frustration for issuers and merchants, who lose the associated revenue when transactions are declined, and cardholders, who are at best inconvenienced and at worst embarrassed. Nearly one-third of shoppers say they've abandoned a purchase entirely or gone to a competitor after being wrongly declined.

Removes friction. In global markets where 3DS security protocol is mandated or prevalent, dCVV2 dramatically limits the need for step-up authentication. Because dynamic security codes integrate into the 3DS protocol, transactions are validated with dCVV2 without the need for one-time passwords or telephone calls to the issuing bank. The result is a smoother, more streamlined customer experience.

Lower costs for card issuers. dCVV2's elimination of fraud can help card issuers save on the associated costs they incur in the form of fraud investigation, customer service, replacement cards, reduced card usage and customer attrition.

How dCVV2 complements fraud prevention solutions

dCVV2 fills the security gap left by tokenization, 3DS and AI/ML.

Tokenization

What to know: Tokenization is similar to encryption in that the information transmitted isn't the cardholder's actual card data but random code that maps back to the data. Tokens are issued once for a specific card PAN/merchant combination and can't be used anywhere else. As a result, tokens do a great job of protecting data. They guard against data breaches, whether the data is at rest on the merchant site or in transit.

The major drawback to tokenization is that it doesn't protect consumers from fraud. That is, it does nothing to prevent stolen card data – PANs, expiration dates and CVV codes – from being used. Fraudsters can shop online and pay for their purchases with stolen cards that merchants then convert into tokens. The result? The fraudster now has a token of a stolen card. And all the tokenization in the world won't prevent enumeration attacks because consumers' credentials remain valid.

Tokenization similarly falls short in protecting against the rise of digital skimming, also called web skimming or e-skimming. In digital skimming, fraudsters compromise websites' payment or checkout pages by injecting malicious code that creates realistic-looking fake screens to capture card details. Digital skimming has become a preferred method of capturing credit card data, with the number of reported cases increasing 174% between June and November 2022, compared to the period between December 2021 and May 2022.

How dCVV2 fills the gap: Tokenization protects data; dynamic security codes protect the cardholder. They safeguard against theft of the card. The code itself becomes a moving target: Even if fraudsters successfully steal payment credentials, the security code stops working within hours.

dCVV2 prevents fraud on tokens issuance. Token vaults issue tokens based upon the card details initially provided, by validating dCVV2 at the time of token issuance, stollen card details are prevented from becoming fraudulent tokens, and the resulting fraud can be prevented.

3DS

What to know: 3DS is widely used—and still struggling to shake off its sluggish start 20 years ago. The global security protocol works best as part of a multi-level fraud prevention strategy. Its use is mandated in Europe and several other countries such as Nigeria, Singapore, and South Africa. 3DS is not mandated in the United States, although it has been implemented by large e-commerce vendors such as Walmart. Estimates are that 35% of merchants globally use 3DS.

Yet 3DS falls short in several areas. For one thing, merchants are required to initiate the process, limiting the scope of the protocol's fraud prevention. It is also relatively expensive and impractical for small purchases. In Europe transactions under 30 euros are exempt from 3DS authentication, leaving low-value purchases unprotected—and cardholders vulnerable.

In addition, customer experience is fragmented. There are many variations in how 3DS is executed. Risk scoring continues to produce false positives, and the challenge experience varies by bank: Some cards challenge cardholders via text message; others require a phone call.

Detractors say 3DS's high rate of challenges adds up to not only a poor CX but also lost sales for merchants. The industry continues to debate whether 3DS is a "conversion killer."

Equally important, 3DS does nothing to prevent first-party or friendly fraud—fraudulent activity by a consumer rather than a fraudster. Authenticating customers prior to purchase offers no protection for friendly fraud, which accounts for the bulk of merchants' chargebacks.

How dCVV2 fills the gap: dCVV2 requires no merchant enrollment and protects all transactions, even zero-dollar transactions, not just those over 30 euros. It improves the 3DS CX by validating dCVV2 within a 3DS (2.3) step-up and eliminates the need to challenge the cardholder. The result is a better cardholder experience.

During authorization the implementation of dCVV2 results in a 3.5% increase in approvals, which equates to an 85% reduction in false positive transaction declines.

AI/ML

What to know: AI and machine learning (ML) systems excel at churning through enormous volumes of data, a capability that's critical to the fraud prevention ecosystem—and still several years off.

ML models' specialty is detecting complex, subtle patterns among datasets that include transactions, user behavior, and analytics. The AI algorithms at the heart of ML adapt quickly—a trait that puts the AI/ML combination far ahead of traditional rule-based systems when it comes to payment fraud and facilitating advances like real-time monitoring. Those qualities make AI algorithms good at reducing false positives and false negatives (fraudulent transactions that the system misses) as well as spotting friendly fraud.

But AI/ML's learning strengths are also potential weaknesses: The technology's output is only as accurate and reliable as the data fed into the models, so low-quality or incomplete data will lead to skewed outcomes. Biased data is a critical risk factor for fraud prevention, with increased false positives and false negatives leading to financial losses for businesses.

Equally threatening, fraudsters may attempt to manipulate AI models by generating patterns that bypass detection. Adversarial attacks pose a challenge to maintaining AI systems' integrity and effectiveness.

How dCVV2 fills the gap: Like other fraud technologies, AI and ML don't do anything to stop the actual data breach. If a fraudster has the cardholder's details, the card will still work. Dynamic security codes complement AI and ML by safeguarding the security code and through two-factor authentication.

Overview of Issuer CNP Fraud Prevention Solutions

SOLUTIONS

THREATS	3D secure	Tokenization	DAF/TAF	Risk based (AI/ML)	Dynamic CVV2
OVERALL	◔	◔	◔	◔	◕
Stolen card data	◔	○	◔	◔	●
Stolen card	○	○	◔	◔	●
Enumeration attacks	○	○	○	◔	●
Data breach at merchant	◔	●	●	◔	●
Account takeover	◔	○	○	◔	◑
Social engineering	◔	○	◔	◔	◑
Friendly fraud	◔	○	○	◔	◑
Biometrics	✓		✓	✓	✓
Customer experience	☹	☺	☹	☺	☺

Very effective ● **Ineffective** ○

Source: Keyno 2022

A combination of complementary solutions delivers the most significant reductions in fraud:

- Tokenization to secure data at merchants
- Dynamic CVV2 to prevent fraud from stolen card/card data and enumerations attacks
- Advanced Risk-Based Authentication using AI/ML to prevent fraud from account takeover, social engineering, and friendly fraud

For issuers currently using 3DS, adding Dynamic CVV2 improves the customer experience and reduces fraud significantly

Conclusion

For card issuers, the CNP fraud challenge shows no signs of letting up. As a result, successful fraud prevention is a key business objective. dCVV2 technology helps to meet that objective with a digital solution that provides the security cardholders are looking for. It complements existing security measures like tokenization, 3DS and AI/ML by offering protection when stolen card credentials are in the fraudsters' possession. The result is a user experience that leaves cardholders feeling safer online and in greater control of their card usage.

References

1. The Nilson Report, Payment Card Fraud Losses Reach $32.34 Billion, December 22, 2022

2. Mastercard and Network International launch new AI fraud-prevention solution, February 2023

3. January-June 2022, LexisNexis 2022 Global State of Fraud and Identity Report.

4. The Nilson Report, Payment Card Fraud Losses Reach $32.34 Billion, December 22, 2022

5. Recorded Future, Annual Payment Fraud Intelligence Report: 2022

KEYNO

Keyno replaces the static 3-digit CVV2 security code on the back of your current credit, debit or prepaid cards with a continually changing "dynamic" CVV2 code that hackers and scammers can't capture and use. Keyno sends a new code every 4-12 hours to your smartphone, keeping your cards safe. Keyno sends a continually changing 3-digit CVVkey code to smartphones to outwit would-be fraudsters. Getting a fresh 3-digit code is as simple as glancing at your phone.

Have questions about how Keyno works? **Email us** and we'll get back to you with the answers or visit us online at **www.keyno.io**.