PAYMENT SECURITY SOLUTIONS GUIDE

A Sustainable Approach for Businesses to Mitigate Card Not Present Fraud

AMERICAN EXPRESS

DON'T *do business* WITHOUT IT

Balancing fraud prevention with multi-layered security solutions

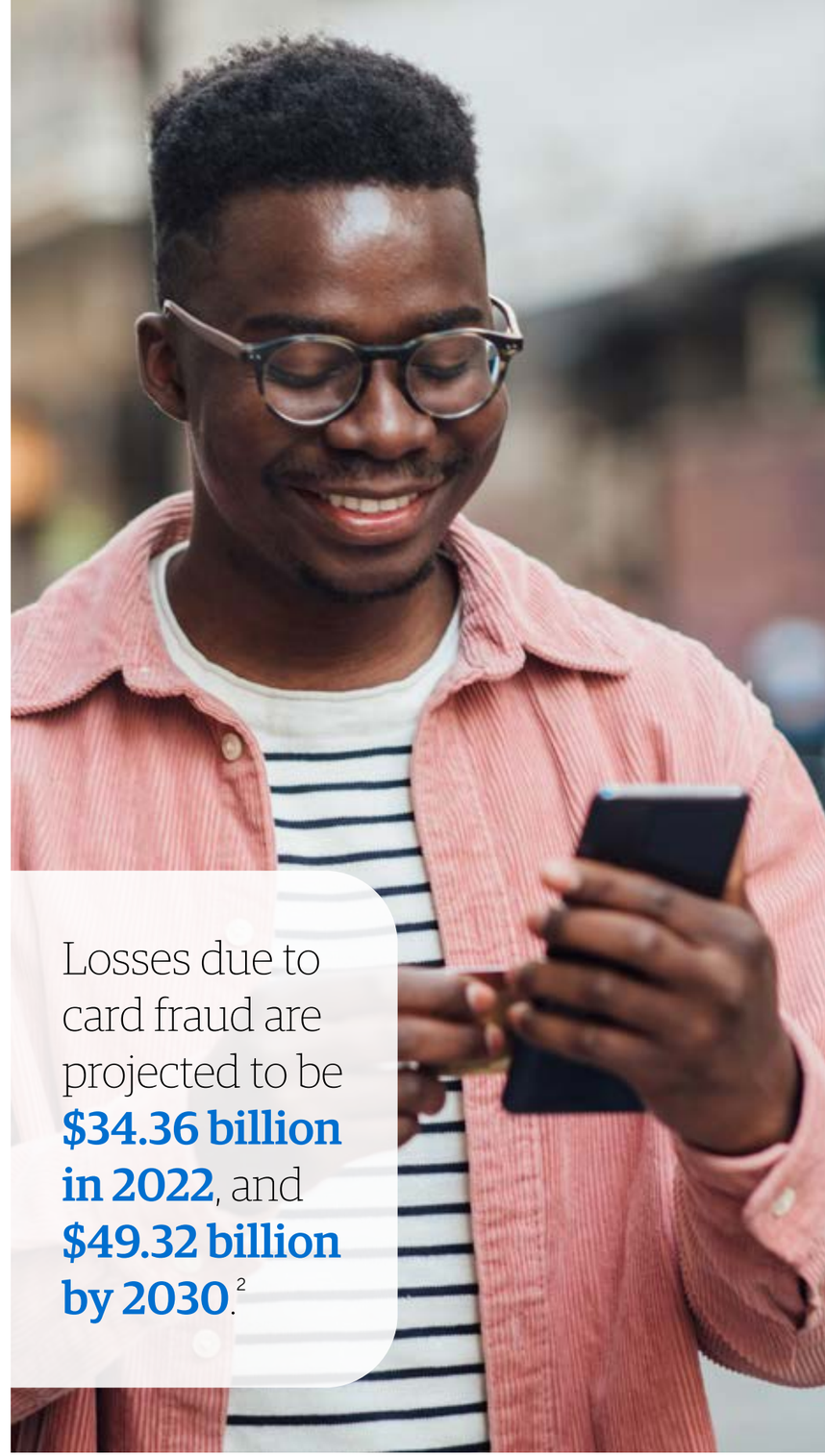
Card not present (CNP) payments continue to increase as e-commerce and online shopping see tremendous growth. By all indications, this trend will only continue in the months and years ahead. According to *Insider Intelligence*, **global e-commerce sales are estimated to reach $5 trillion in 2022** and are expected to grow to **$6 trillion just two years later in 2024**. In the U.S. alone, retail e-commerce sales will grow 16.1%, reaching $1.06 trillion in 2022.[1]

This is great news for merchants, but it comes with a warning: Where e-commerce thrives, fraud often follows.

Fraudsters continue to find new ways to steal card credentials and commit unauthorized transactions, costing businesses billions every year. **Dollars lost to CNP fraud were more than six times higher in 2020 than the prior year**, and it appears this is just a beginning. Losses due to card fraud globally are projected to increase from $32.2 billion in 2021 to $34.36 billion in 2022, and $49.32 billion by 2030.[2] This does not even account for the reputational damage caused by fraud, which is difficult to quantify.

With the heightened pressure to do more to effectively manage this growing threat, you will want to focus on continuously improving your fraud mitigation strategies by leveraging scalable solutions that can help you create multiple layers of protection. In the process, you can maximize revenues through increased approval and fraud detection rates, fewer chargebacks, and decreased false positives.

This guide provides timely information to help you evolve your strategy around payment security. It discusses the current CNP landscape, the types of fraud and techniques used by fraudsters to watch out for, and the Payment Security Solutions from American Express that provide businesses with a sustainable, multi-layered arsenal of solutions to help combat CNP fraud.



Losses due to card fraud are projected to be **$34.36 billion in 2022**, and **$49.32 billion by 2030**.[2]

[1] Ecommerce Statistics: Industry benchmarks & growth, Insider Intelligence, January 2022.
[2] Issue 1209, Nilson Report, December 2021.

Fraud comes at you from many directions

Fraudsters keep evolving the methods they use to illicitly obtain payment information and conduct fraudulent transactions. To better understand the problem, let's look at the two most common techniques for illegally procuring payment credentials, as well as the top two forms of fraud abuse.

Favorite data theft techniques

A **cybersecurity breach** is an incident wherein an attacker gains unauthorized access to computer data or networks over the internet without the knowledge of the system's owner, resulting in exposure and theft of sensitive, protected, or confidential information. Most cybersecurity breaches are accomplished by hacking or malware attacks.

IBM's Cost of a Data Breach Report 2021 found that the **average total cost of a data breach increased by nearly 10% year over year**, the largest single-year cost increase in the last seven years.[3] Lost business represented the largest share of breach costs, at an average total cost of $1.59 million, and overall, **cost averages rose from $3.86 million to $4.24 million**, the highest in the 17-year history of the report.

Phishing/Smishing are methods fraudsters use to trick targeted recipients into giving them personal financial information. Phishing uses emails to gather that information, while smishing is implemented through text messages or SMS, hence the name "SMiShing." Messages appear to come from a reputable source, such as the recipient's financial institution, and typically request personal information such as passwords and credit card credentials to "update" or "validate" an account.

According to CISCO's 2021 Cybersecurity Threat Trends Report, about **90% of data breaches occur as a result of phishing**. IBM's 2021 Cost of a Data Breach Report identified phishing as the second most expensive attack vector, at an **average cost of $4.65 million per business**.[4]

[3] Cost of a Data Breach Report, IBM, 2021.
[4] Cybersecurity threat trends: phishing, crypto top the list, Cisco Umbrella, 2021.

Most common fraud techniques

A **compromised payment credential** is stolen credit card information that is used to make purchases and conduct transactions, usually online.

The IBM report found that customer Personally Identifiable Information (PII) was **the most common type of record lost or stolen**, with 44% of PII included in all breaches.[5] In a survey conducted by American Express, more than one in five respondents experienced a fraudulent attempt to use their credit card or payment information. One in 10 had their credit/debit card stolen in the past year. [6]

An **account takeover** is a form of identity theft and fraud where a malicious third party successfully gains access to a user's account credentials, often by purchasing stolen usernames and passwords on the dark web, to make unauthorized transactions, withdraw money, redeem reward points, or use the information to access other accounts.

Quoting from the Nilson Report, "Account takeovers by fraudsters buying card credentials on the dark web have become a bigger problem the past few years. Stolen [card information] can be bought on the dark web for as little as $5.80, on average, and **the U.S. has the most stolen cards circulating.**"[6]

[5] The Privacy Paradox: Securing Data To Build Customer Engagement, PYMNTS.com, August 2021.
[6] The 2021 American Express Digital Payments Study, American Express, May 2021.
[7] Card industry faces $400B in fraud losses over next decade, Nilson says, Payments Dive, December 2021.

The consequences of fraud add up

The impacts of CNP fraud can range widely. They can be felt immediately, or they can go undiscovered for long periods of time. **In 2021, it took an average of 212 days to identify a cybersecurity breach, and an average of 75 days to contain it.**[3] That means the damage to the customer was likely done before any action could be taken to prevent it.

Nilson estimates that **issuers, merchants, and acquirers lost at least $28.58 billion globally last year.**[7] Actual losses likely exceed that amount, however, due to expenses related to fraud investigation, managing call centers, and maintaining operations, which tend to rise annually. Additionally, the cost of fraud and associated chargebacks can be expensive not only in monetary terms but can also cause longer term reputational damage that may impact future business.

All told, **card industry losses to fraud over the next 10 years are estimated to collectively reach $408.50 billion**, according to the December 2021 Nilson report.

As these consequences escalate, it becomes imperative to use mitigation strategies that employ multiple ways of ensuring validity of transactions and Card Member authentication. Adding a variety of checkpoints during and after the transaction lifecycle will help minimize risk and reduce the impact of fraud. And using technologies that have been tested and proven effective can help ensure that the strategy is sustainable and scalable as your business grows.

Merchants are taking steps to reduce their vulnerability and keep their customers safe.

58% of merchants offer enhanced security requirements at checkout to help protect customer card information.

Another **21%** plan to adopt more enhanced requirements in the next 12 months.[8]

[3] Cost of a Data Breach Report, IBM, 2021.
[7] Card industry faces $400B in fraud losses over next decade, Nilson says, Payments Dive, December 2021.
[8] Digital Convenience is Here to Stay, American Express, 2021.

The American Express Payment Security Solutions Suite

A MULTI-LAYERED, SUSTAINABLE APPROACH TO FRAUD PREVENTION

Using our unique expertise as a global Issuer, Acquirer, and Payment Network, American Express provides tested and proven solutions that can help you integrate a multi-layered approach to fraud prevention while supplementing your current solution set.

Our Payment Security Suite of Solutions is built on industry standards and ranges from fraud prevention to customer and transaction authentication to help you mitigate fraud more effectively.

KEY BENEFITS MAY INCLUDE:

- Reducing risk and exposure to fraud
- Increasing approval rates
- Decreasing cost of fraud
- Avoiding declined authorizations
- Improving customer experience
- Protecting customer data

Enhanced Authorization

SafeKey 2.0

Card-on-File Tokenization

Verify-It

Accertify

All products and services may not be available to all merchants and regions.
Please contact your American Express representative to learn more about availability.

Enhanced Authorization

REDUCE FRAUD UP TO 60%

By enabling you to share additional transaction data with American Express, Enhanced Authorization works behind the scenes to help you better identify who is on the other side of the transaction in real-time. Use of machine-learning models and analytical tools improve our ability to assess risk and distinguish between a legitimate customer and a fraudster.

KEY BENEFITS MAY INCLUDE:

Increasing approval rates. Legitimate customers are more easily identified through sharing of additional information.

Decreasing false positives. Customers who may have been declined in the past may now get approved due to improved risk assessment.

Improving the customer experience. There is no impact on customer checkout, no step-up authentication—you provide data elements in the background, in the authorization request.

Achieving up to 60% reduction in fraud. Because Enhanced Authorization can help American Express to identify legitimate customers, we can also more accurately decline fraudulent attempts.

Enhanced Authorization

USE CASE

PROBLEM

Merchants of all sizes may see an increase in declined transactions due to suspected fraud, likely turning away a good number of legitimate sales.

SOLUTION

Enhanced Authorization delivers more accurate authorization in real-time for an improved response. Merchants can capture and send incremental transaction data to American Express behind the scenes of a transaction. American Express compares the data against positive and negative usage across the Network and other data sources, then incorporates the data into the authorization decision. With this solution, the Merchant can reduce fraud and avoid unnecessary declines.

CONSIDERATIONS

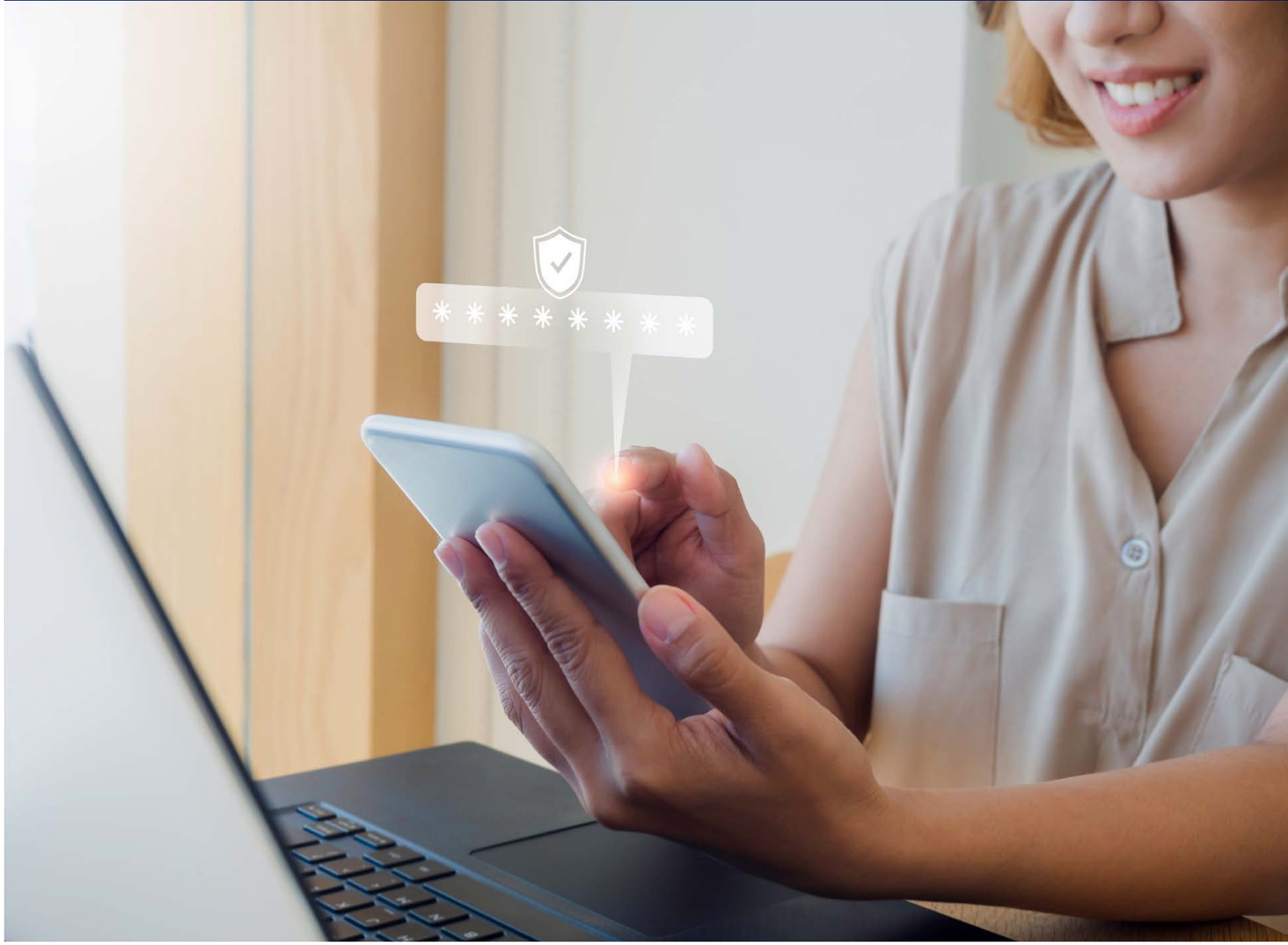
Enhanced Authorization is available globally only to Merchants that have a direct contractual relationship with American Express. Although provided by American Express at no cost to the Merchant, some tech investment may be required.

Learn more about Enhanced Authorization. To get started, contact your American Express representative.

SafeKey 2.0

PREVENT FRAUD WHILE REDUCING FRICTION DURING CHECKOUT

American Express SafeKey 2.0 leverages the global industry standard EMV®* 3-D Secure to provide an additional layer of security for your customers shopping through web browsers or making in-app purchases. It enables you and the Issuer to exchange detailed customer information to validate their identity, limiting the need for using verification methods such as a one-time passcode to high-risk transactions, thereby reducing transaction friction for a safe and a seamless checkout experience. Furthermore, SafeKey 2.0 transfers liability to the Issuer for fraud chargebacks on authenticated and attempted transactions.



KEY BENEFITS MAY INCLUDE:

Decreasing your fraud liability. Transfers liability for fraud chargebacks on authenticated and attempted transactions to the Issuer.

Increasing your customers' spend confidence. By providing them with added security to their online purchases.

Reducing shopping cart abandonment. Risk-based authentication techniques are used to limit the use of stronger authentication methods such as one-time passcodes for high-risk transactions, reducing friction and leading to higher conversion of sales.

*EMV 3-D Secure is a product of EMVCo, which is the global technical body that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Specifications and related testing processes.

On average, 85% of transactions decisioned using SafeKey 2.0 do not require a challenge (such as a one-time passcode) at checkout, thereby reducing friction for most transactions.

Based on internal American Express proprietary data, May – November 2021.

SafeKey 2.0

USE CASE

PROBLEM

Merchants with growing businesses often experience increasing costs related to chargebacks caused by fraud. While Merchants want to prevent fraud proactively, they want to do so using techniques that present minimal friction to customers.

SOLUTION

With enhanced data exchange, SafeKey 2.0 enables the Issuer and Merchant to work together to authenticate the customer's identity, improving the Issuer's confidence to authorize the transaction, while reassuring the Merchant and protecting their bottom line by shifting fraud liability to the Issuer.

For the customer, SafeKey 2.0 reduces friction by limiting the need to invoke the use of additional verification such as a one-time passcode to transactions determined as high risk. This can help reduce shopping cart abandonment for the Merchant, leading to higher sales conversion.

CONSIDERATIONS

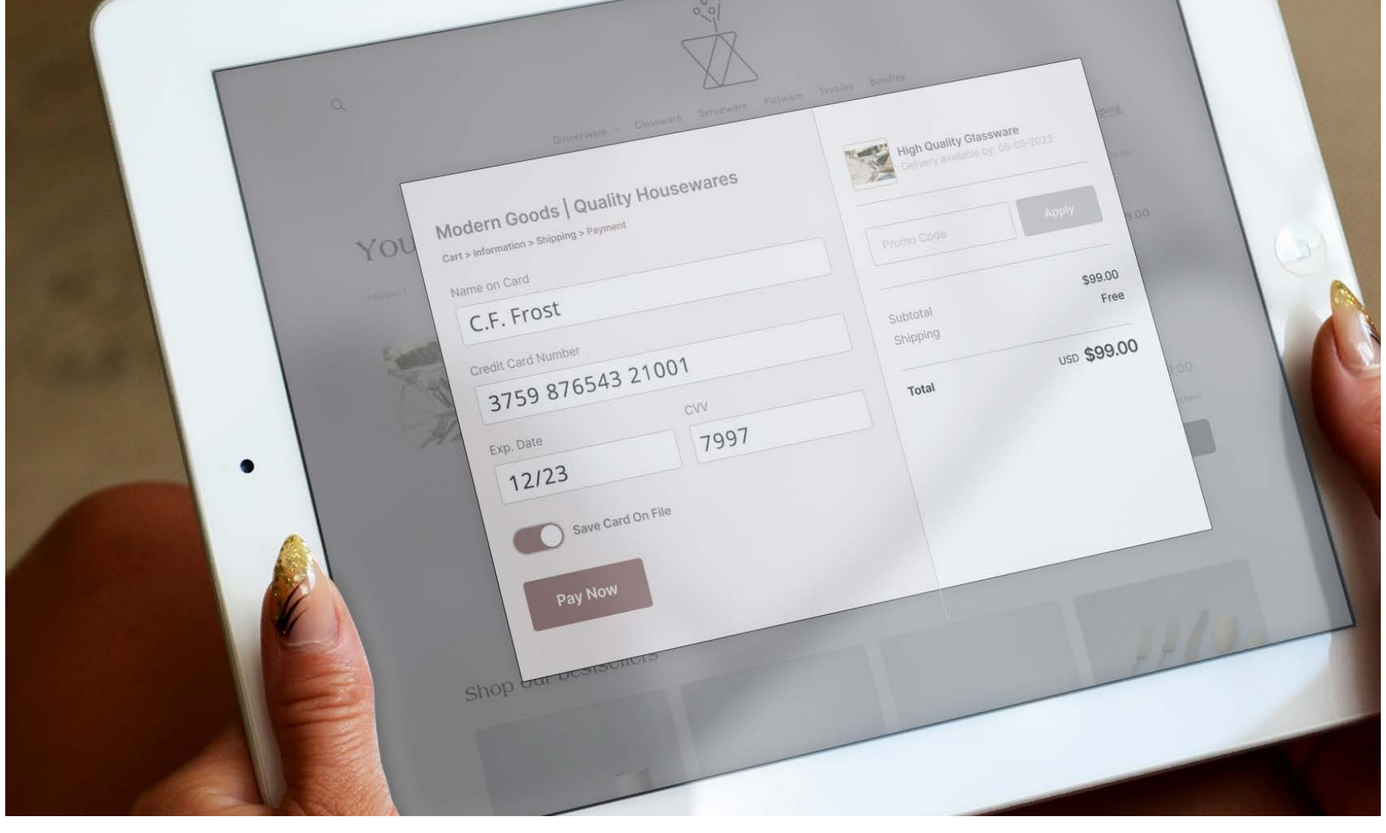
Available to all Merchants globally, at no charge from American Express to the Merchant. However, to enable SafeKey, Merchants need to work with a service provider who may charge for the service.

Learn more about SafeKey 2.0.
To get started,contact your American Express representative.

Card-on-File Tokenization

PROTECT YOUR CUSTOMER AND YOUR BUSINESS

Card-on-File Tokenization (CoFT) from American Express provides additional security when your customers save their payment credentials online for future transactions. It replaces their actual Card numbers (Primary Account Number/PAN) with payment tokens—a series of randomly generated numbers, which helps prevent its unauthorized use. Using payment tokens can help you secure sensitive payment information and keep Card credentials associated with the tokens up to date when Cards get replaced.



KEY BENEFITS MAY INCLUDE:

Reducing risk of fraud. Since payment tokens are a string of randomly generated numbers, they are meaningless to fraudsters and hackers, adding security to online transactions and reducing the risk of fraud. Storing tokens instead of Card information may limit the scope of PCI DSS compliance.*

Improving authorization rate. Use of domain controls for payment tokens can give Card Issuers greater confidence to authorize transactions.

Avoiding revenue stream disruptions and declined authorizations. Card credentials are automatically updated for associated tokens when Cards are replaced and tokens are used to process transactions.

Providing a seamless customer experience. Customers can quickly complete the online checkout process and continue uninterrupted when payment tokens are used to process transactions.

Minimizing build and compliance costs. Storing payment tokens instead of Card credentials may reduce the costs associated with PCI compliance reviews.

*Please refer to the PCI DSS requirements to check whether this applies to your organization.

According to a recent American Express survey, 93% of businesses surveyed that currently store PANs only are likely to consider tokenization for Card-on-File customers in the future, with 53% very likely to consider it.

American Express survey conducted December 1-13, 2021, among a sample of 411 U.S. businesses with $250 million and above in annual revenue.

Card-on-File Tokenization

USE CASE

PROBLEM

Merchants with businesses that typically see customers return for frequent purchases or offer services that require recurring billing often provide customers with the option to save their Cards on file. To encourage customers to save their payment credentials, Merchants need to be able to assure their customers that their information will be secure, along with the added benefit of eliminating the friction of manually inputting new Card-on-File data when Cards are replaced.

SOLUTION

Merchants can secure the customer's payment credentials by enabling CoFT, which will replace it with a token issued through the American Express Token Service (AETS) and send it to the Merchant, who stores the token in place of the customer's account number for future use. Additionally, when a Card gets replaced, the Card information associated with the payment token is automatically updated, ensuring that the payment process continues uninterrupted.

CONSIDERATIONS

American Express utilizes its EMVCo registered Tokenization Service to support provisioning of tokens, providing security as an industry-recognized Token Service Provider (TSP). Click here to see if CoFT is available in your country.

As a Merchant, you can choose from two models to enable CoFT:

1. **Token Requestor Model:** Best suited for Merchants who submit authorization transactions directly to the American Express Network without a third-party partner.
2. **Token Requestor Aggregator Model:** Best suited for Merchants who use a third-party partner to store their customers' Card credentials and to submit transactions on their behalf.

Learn more about Card-on-File Tokenization.
To get started, contact your American Express representative.

Verify-It

QUICKLY VALIDATE CUSTOMER INFORMATION WITH 24/7 SUPPORT

This browser-based security tool can help your business minimize fraud when processing online orders. It allows you to quickly validate billing name and address information to easily identify high-risk transactions that may require additional verification. Verify-It helps you make real-time decisions on order fulfillment before shipping, 24 hours a day, seven days a week. You can also use it to support fraud or security investigations, as well as chargeback research efforts.

KEY BENEFITS MAY INCLUDE:

Being easy to use and cost effective. Simple registration process and no software to download or install.

Saving valuable time and helping reduce exposure to fraud. Verify-It can help you quickly make real-time decisions on order fulfillment by checking the Card information provided on an order against the customer-level information on file with American Express.

Verify-It

USE CASE

PROBLEM

Merchant struggles with secure verification of “riskier” phone or online orders such as larger-than-normal transactions or new customers.

SOLUTION

Verify-It provides that one last check before orders go out the door. After the Merchant enters the Card Member name, address and phone number related to an order through the Verify-It global web portal, Verify-It checks it against the Card Member account information on file with American Express to help Merchants identify high-risk transactions and make real-time decisions before shipping.

CONSIDERATIONS

Verify-It is available globally to eligible Merchants that have a direct contractual relationship with American Express and there is limited availability for all other Merchants, at no cost.

Learn more about Verify-It.
To get started, contact your American Express representative.

Accertify

MITIGATE FRAUD AND ABUSE ACROSS THE ENTIRE CUSTOMER JOURNEY

Accertify, a wholly owned subsidiary of American Express, is a leading solutions provider for payment fraud and abuse, chargeback management, digital identity, device intelligence, and payments. Founded by former in-house fraud and risk managers, Accertify's suite of products and services is a layered risk platform with machine learning and rich reputational community data that helps the leading global retail brands, the top five global airlines, and key financial service providers apply multiple layers of defense to combat fraud. Accertify can protect you and your customers from the ever-increasing online risks across all your Card brands.

KEY BENEFITS MAY INCLUDE:

Maximizing revenue. Improved detection rates, fewer chargebacks, and decreased false positives.

Driving down the total cost of fraud. Decreases fraudulent account openings and takeovers.

Improving authorizations. Helps reduce false positives without the need for additional manual review.

Using the unmatched power of community data. Leverages community data and industry-specific machine learning models to provide insights for all transactions across retail, airlines, travel, ticketing, entertainment and more.

Accertify

USE CASE

PROBLEM

An enterprise-level Merchant, such as an airline, finds an increase in fraudulent transactions originating through ecommerce channels that requires the redirecting or hiring of extra resources for manual reviews. This labor-intensive and time-consuming process can lead to poor user experience and fulfillment delays.

SOLUTION

Accertify can provide large companies with a holistic strategy to managing fraud, instead of a piecemeal approach. Accertify protects 40% of the top 100 online Merchants, eight of the top 10 global airlines and over 350 enterprise customers worldwide. As a result, Accertify helps its customers formulate a clear risk profile of data across many industries and interactions, spotting patterns and anomalies as they arise and then sharing that insight across its network. Accertify enterprise-level community data can provide deep insights across all your transactions to protect against fraud.

CONSIDERATIONS

Available globally to all eligible Merchants and applicable across all Card brands. It is best suited for Merchants with a large and growing ecommerce business. License and software implementation costs apply.

Learn more about Accertify.
To get started, contact your American Express representative.

A Multi-Layered Approach

PUTTING IT ALL TOGETHER

The Payment Security Solutions Suite from American Express provides multiple layers of defense to combat fraud. By taking this approach, you can maximize revenues through improved fraud detection rates, increased approval rates, fewer chargebacks, and decreased false positives. You can also simplify processes and procedures for preventing digital fraud, and stay one step ahead of fraudsters with the latest features and functionality these solutions provide. Most importantly, you can protect your customers and your business with an interlocking web of defense that can identify fraud before it happens.

USE CASE

PROBLEM

Merchant with a growing online business wants to maintain a frictionless checkout for their customers but is worried about larger-sized transactions. The Merchant is also concerned about exposing customer information in the event of a data breach, and the costs of reputational damage that accompanies an attack.

SOLUTION

The Merchant adopts a strategy that involves the use of multiple solutions, each acting as an additional layer of security.

Enhanced Authorization provides behind the scenes protection, while SafeKey 2.0 allows the customer to provide more information (such as a one-time password), effective for larger transactions. Enhanced Authorization and SafeKey 2.0 leverage additional data elements to instill a greater confidence in authorization decisions.

Another checkpoint can be added prior to shipping very high value transactions by using Verify-It to corroborate the information submitted against the Card Member account information on file with American Express.

To allay concerns surrounding the impact of a data breach, the Merchant can enable the use of payment tokens with Card-on-File Tokenization that protects the anonymity of this sensitive data, should it be exposed.

PAYMENT SECURITY SOLUTIONS

Considerations going forward

While there are many options available to you to help detect and prevent fraud, the optimal strategy includes a set of solutions that addresses the unique need of your business and future proofs it for growth. Here are a few considerations to help you think through the best set of solutions for supporting your strategy and solution framework.

- **Connect with your American Express representative** to help determine where the fraud is coming from and identify high fraud activities that impact your bottom line.
- **Calculate the dollar impact** of fraud activities and identify the areas that would have the maximum impact on your business.
- **Identify potential solutions** and evaluate their probable effectiveness.
- **Shortlist potential solutions and partners** to determine the budget that complements your overall fraud prevention strategy.

Fighting fraud on every front

There is no silver bullet to prevent fraud. However, there are actions you can take to detect and insulate your businesses from future attacks while balancing payment security with customer convenience.

- **Add multiple layers of protection** to help ensure that your payment systems and software are secure and that fraudulent transactions are identified accurately and not authorized.
- **Maintain a secure environment** by adhering to the Payment Card Industry (PCI) Data Security Standard.
- **Leverage the Fraud Classifier℠ model**, recommended by a Federal Reserve-led industry work group, to help consistently classify and better understand the nature and magnitude of fraud.
- **Future proof your business by developing a strategy** that is sustainable, scalable, and includes a layered approach to securing payments.

You are already one-step ahead due to the valuable information you have about your customers and transactions. Combining the data in-hand along with a multi-layered approach, you can create a strong framework for detecting and preventing fraud.

There is no one solution that can do it all and there is no cookie cutter approach to payment security. Every business is unique, and their situations and objectives vary. By analyzing the risks faced by your business and the associated costs, you can find opportunities and solutions that reduces fraud and can help your business flourish.

Learn more about Payment Security Solutions from American Express.
Visit our website and connect with your American Express representative today.

Resources

[1] Ecommerce Statistics: Industry benchmarks & growth, Insider Intelligence, January 2022. insiderintelligence.com/insights/ecommerce-industry-statistics

[2] Issue 1209, Nilson Report, December 2021. nilsonreport.com/upload/content_promo/NilsonReport_Issue1209.pdf

[3] Cost of a Data Breach Report, IBM, 2021. ibm.com/security/data-breach

[4] Cybersecurity threat trends: phishing, crypto top the list, Cisco Umbrella, 2021. umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

[5] The Privacy Paradox: Securing Data To Build Customer Engagement, PYMNTS.com, August 2021. pymnts.com/study/privacy-paradox-data-security-customer-engagement-personal-information

[6] The 2021 American Express Digital Payments Study, American Express, May 2021. Research Method: The 2021 American Express Digital Payments Study is based on a sample of 1,002 respondents weighted to U.S. census based upon gender, age, education, race and region. Unless otherwise noted, responses among consumers represent those who have made an online purchase three or more times in the past 12 months based on self-report. The anonymous survey was conducted online May 21-23, 2021.

[7] Card industry faces $400B in fraud losses over next decade, Nilson says, Payments Dive, December 2021. paymentsdive.com/news/card-industry-faces-400b-in-fraud-losses-over-next-decade-nilson-says/611521

[8] Digital Convenience is Here to Stay, American Express, 2021. Research Method: The Amex Trendex: 2021 Digital Payments Edition is based on a sample of 1,002 respondents weighted to U.S. census based upon gender, age, education, race and region. The anonymous survey was conducted online May 21–23, 2021. The business survey is based on a sample of 400 business leaders in the U.S. who have responsibility for making decisions regarding customer payment options, IT/data security, or online sales strategy and planning. Respondent companies must offer credit/debit card or digital payment options to their customers in addition to online/mobile payment. The anonymous survey was conducted using an online panel July 16–21, 2021. network.americanexpress.com/globalnetwork/dam/jcr:933b52e4-7b41-40e2-995c-3691cc1efd90/Amex%20Digital%20Trendex%202021%20Digital%20Payments%20Edition.pdf