

Balance Security with a Frictionless Online Shopping Experience for Your Cardholders

Payment security solutions from CA Technologies help issuers overcome obstacles by offering zero-touch authentication to their cardholders. By migrating to a solution that allows issuers to implement a flexible and dynamic 3D Secure program combined with neural network 3D Secure authentication models for continual Risk-based assessment, issuers can more effectively combat e-commerce fraud without negatively impacting the cardholder's online shopping experience.

Business Challenges

Where There Is Opportunity, There Is Risk!

- E-commerce is growing at an unprecedented pace, with mobile commerce alone expected to climb to \$626B in 2018. Right alongside there, banks face similar growth in e-commerce fraud as well as pressure from alternative payments. In the US alone, fraud losses will reach over \$7.2B for card-not-present transactions by 2020.
- To compete, you must capitalize on this opportunity and employ innovative technology that will future-proof your organization from all types of fraud; all while providing a frictionless customer experience for your cardholders.
- Today, 3D Secure has nearly reached critical mass but still continues to grow, offering a huge opportunity for issuers. 3D Secure is now much more sophisticated and provides issuers with unique data about customer online shopping habits such as device location, merchant URL, connection speed and much more.
- By adding continual Risk-based assessment (via neural network authentication models) to supplement 3D Secure's effectiveness, issuers can gain the flexibility and control to make the most complex transactions frictionless.

For more information, please visit

<http://www.ca.com/us/products/payment-security.html>

Payment Security Solutions from CA Technologies

"Zero-touch Authentication" can help decrease card-not-present (CNP) fraud losses, increase revenue and acceptance rates, reduce operational costs and improve the overall online shopping experience.



Increased Acceptance Rate

Frictionless shopping leads to interchange and net interest income.

Reduction in Fraud

Improving the false positive ratio with best-in-class neural network authentication models.

Reduction in Operational Costs

Greater accuracy in fraud detection leads to a reduced number of inbound calls and cases.



Key Benefits and Results

- **CA Transaction Manager** allows issuers to offer a flexible and dynamic 3D Secure program to their cardholder, helping to effectively combat ecommerce fraud.
- **CA Risk Analytics** transparently assesses the fraud risk of an ecommerce transaction in real-time during authentication.
- **CA Strong Authentication** for Payments is a cloud service that provides issuers the freedom to offer various methods of strong authentication, depending on what is necessary and practical for their cardholders.

Marquee benefits yielding **\$1.3M** per year in savings are detailed on the reverse side of this document in order to show examples of business value achievable through this Payment Security approach.

Key Features

- Full compliance with Verified by Visa, MasterCard SecureCode, JCB/J/Secure, American Express SafeKey and Discover/Diners ProtectBuy cardholder authentication programs.
- Supports individual banks, global banks, service providers and processors who offer card management services. The flexible architecture facilitates integration with existing card issuer systems including home banking and fraud management systems.
- Accurately determines whether or not a transaction is legitimate or fraudulent, allowing the majority of cardholders to continue with their purchase without unnecessary intervention.
- A comprehensive case management system allows immediate access to fraud data so that analysts and customer support representatives can prioritize and take action on cases, query fraud data and manage alerts
- Provides several mobile authentication options including push notifications, OTP via SMW/email and a mobile OTP app. Issuers have the freedom to choose whichever method of strong authentication they would like to employ, depending on what is necessary and practical for their cardholders.





Business Value Estimations for CA's Payment Security Solutions

Payment Security zero-touch authentication solution benefits can be quantified via a wide range of **CA Transaction Manager**, **CA Risk Analytics**, and **CA Strong Authentication** benefit scenarios. A selection of these is listed below to show common areas measured.



Business Value Proposition	Business Value Enabler	Specific Measurement	Impact ¹ Range	Key Resources Affected	Average ² Resource Value	Projected ³ Savings / year
Increase Revenue and Acceptance Rates	<ul style="list-style-type: none"> By identifying legitimate cardholders and allowing them to proceed directly to checkout, issuers can create a frictionless customer experience, which translates into lower abandonment and failure rates. This is enabled through the ability for issuers to write custom rules, choose from a set of pre-defined rules and leverage neural-network authentication models to accurately separate fraud from non-fraud, allowing only low-risk transactions to proceed directly to checkout. 	Reduction in failed or abandoned transactions	80-90%	Abandoned Transactions ^{4,5}	1,000,000	\$221,000 Interchange Fees \$663,000 Interest Revenue
Deny Fraud Attempts	<ul style="list-style-type: none"> Combining CA's neural-network authentication models with issuer defined rules give issuers the ability accurately identify true fraud and outright deny or enforce step-up authentication. By denying transactions that are accurately identified as high-risk, issuers can stop fraudsters without giving them the opportunity to attempt to pass a challenge request. This reduces the risk of many types of fraud that lead to revenue loss, including account takeover, while impacting fewer legitimate customers 	Improvement in fraud attempts denied	45-55%	Fraud Denied ⁶	\$390,000	\$195,000
Challenge Fraud Attempts	<ul style="list-style-type: none"> For transactions that are deemed medium-risk by CA's neural-network authentication models combined with issuer-defined rules, issuers have the ability to challenge a fraud-rich pool of transactions. By challenging those transactions, issuers can require authentication by the "cardholder," stopping fraudsters while allowing through legitimate cardholders who successfully authenticate. This can reduce the risk of many types of fraud that lead to revenue loss, while impacting fewer legitimate customers. 	Improvement in fraud attempts challenged	25-35%	Fraud Challenged ⁷	\$273,000	\$81,900
Reduce Help Desk Costs	<ul style="list-style-type: none"> Frictionless cardholder experience translates into lower abandonment and failure rates; this leads to fewer inbound calls for transaction issue resolution. Sophisticated case management and highly customized queue management workflows allow CSRs to review authentication history and match case processing to available agent capacity. Issuers can prioritize cases for outbound fraud investigation and focus on the highest priority cases, reducing the cost of fraud investigations. Fraud marking within case management enables managers and analysts to see rule efficacy and use reporting capability to optimize rules and workflow. 	Reduction in in-bound call volume for transaction issue resolution	80-90%	Customer Call Volume ⁸	40,000	\$153,000

This table shows some key benefits of CA's Payment Security solutions. Your CA Technologies representative can also share additional and more detailed ROI business case examples for this solution by engaging the CA Business Value Analytics Team. This team works with CA's customers to develop and analyze a comprehensive set of assumptions and environment specific metrics in order to build customized projective business cases.

¹ The **Impact Ranges** shown above are estimations derived from the analysis of benchmark data which is a composite of data derived from industry analyst published information, interviews with subject matter experts and experiential data from prior projective analyses.

² The **Average Resource** column metrics may be typical of large corporations offering diverse products and services to their customers.

³ **Projected Savings** calculations are based on the product of the midpoints of the Impact Range and Average Resource Value to show a single representative potential savings value. Please note, the values expressed in this table are not a guarantee of achievable results and will vary depending upon your current infrastructure, people, and processes as well as the appropriate, effective implementation, adoption, and use of the CA solution.

⁴ Interchange Fee calculation is based on 1,000,000 annual transactions, average transaction amount of \$130, an abandonment rate of 20% and an interchange fee of 1%.

⁵ Interest Revenue calculation is based on 1,000,000 annual transactions, average transaction amount of \$130, an abandonment rate of 20%, revolving transactions at 40% with a 9 months balance payment delay, and a 10% annual percentage rate (APR).

⁶ Fraud attempts denied calculation is based on 1,000,000 annual transactions, average transaction amount of \$130 and a 0.30% basis points of fraud.

⁷ Fraud attempts challenged calculation is based on 1,000,000 annual transactions, average transaction amount of \$130, a 0.30% basis points of fraud, and a challenge effectiveness rate of 70%.

⁸ Help desk call volume is calculated based on 1,000,000 annual transactions, an abandonment rate of 20%, and an estimate that 20% of abandoned transactions result in help desk calls for issue resolution. Cost per in-bound call used in computation is \$4.50.

