SOLUTION BRIEF
PAYMENT SECURITY

How do I Balance Robust Security with a Frictionless Online Shopping Experience for Cardholders?

ca technologies

Payment Security solutions from CA Technologies can help reduce friction and decrease abandonment in Card Not Present (CNP) transactions by identifying legitimate cardholders and allowing them to proceed directly to checkout. Transactions that are deemed risky can be denied or subjected to step-up authentication.

Executive Summary

Challenge

The explosive growth of eCommerce has focused attention on security concerns associated with online payment transactions. Cardholders worry about the safety of online transactions while card issuers are concerned about balancing the risks and costs of payment fraud with a loss of revenue caused by transaction abandonment. The 3-D Secure protocol allows payment card issuers to reduce fraud in payment transactions by verifying cardholder identity during Card Not Present (CNP) transactions. Before a transaction is authorized, a cardholder can be challenged to enter a password, answer a question, or use some other form of authentication credential. This interruption in the transaction often causes legitimate customers to abandon the purchase resulting in loss of revenue for the issuer. The challenge is how to reduce fraud without impacting the user purchase experience.

Opportunity

The basic 3-D Secure protocol has helped issuers reduce CNP fraud, however there are areas for improvement.

- If cardholder authentication credentials have been compromised, fully-authenticated fraud may occur.
- The 3-D Secure protocol by itself doesn't differentiate between genuine cardholders and fraudsters so all transactions need to be authenticated and cardholders must enroll.
- 3-D Secure provides an interface for authentication but doesn't include strong authentication capabilities.

Payment Security solutions from CA Technologies add robust security to 3-D Secure programs. CA Transaction Manager enables you to implement your choice of 3-D Secure program, Verified by Visa, MasterCard SecureCode, American Express SafeKey and Diners Club ProtectBuy. CA Risk Analytics analyzes CNP payment transactions in real time and determines the likelihood of fraud. You can bypass cardholder authentication challenges for most legitimate transactions and transparently identify potential fraud even if the cardholder's authentication credentials have been compromised. Finally, for those transactions that are deemed risky, you can use CA Mobile OTP to strongly authenticate suspicious transactions.

Benefits

You can achieve the right balance of security and cardholder convenience by implementing layered security for CNP payment transactions. CA Risk Analytics contributes to a frictionless shopping experience while reducing fraud losses and decreasing transaction abandonment. This translates into a better online shopping experience for your customers and a better bottom line for your business.

Section 1:

Fraud Reduction: At What Price?

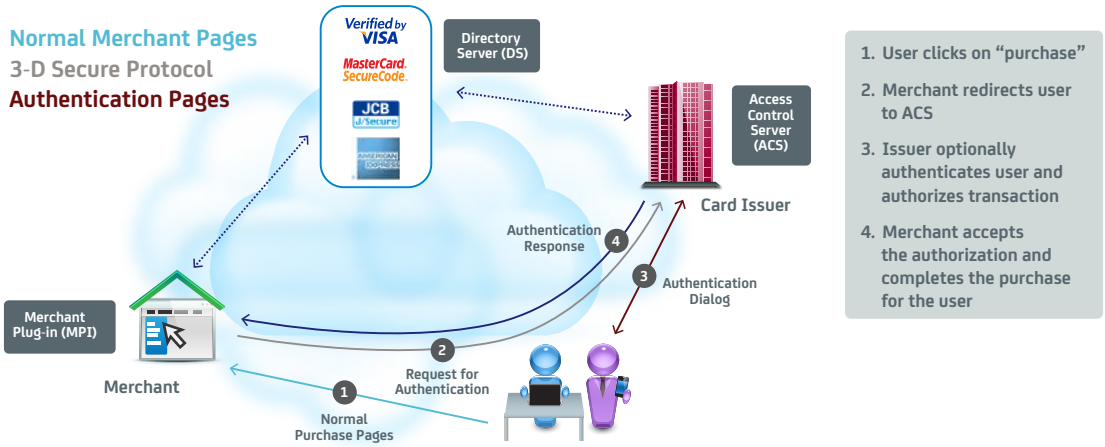
Online shopping is fraught with risk. When a cardholder is using a card online, the normal authentication methods aren't available (viewing driver's license, photo id and signature, or chip-based cards with PIN verification for EMV–compliant payment cards). In addition, the verification numbers on the back or front of the card are not a deterrent if the card was stolen. The primary solution to this problem is 3-D Secure, a service that is designed to make online transactions safer by authenticating cardholders making online purchases. 3-D Secure programs serve to reduce fraud in online transactions, control costly chargebacks and increase customer confidence so they will shop online more frequently. However, the impact of requiring cardholders to enroll in the programs and authenticate has caused an increase in transaction abandonment, which adversely affects issuer interchange revenue. The chargeback process is costly and generally inefficient, which increases the cost of fraudulent transactions above and beyond the actual transaction amount.[1] Today, 3-D Secure services can benefit from a transparent approach to authenticating cardholders during their transactions. Cardholder behavior patterns, devices used, location and other factors can be analyzed in real time allowing the majority of legitimate transactions to continue without any change to the user experience during checkout.

3-D Secure provides the base layer

The 3-D Secure protocol allows payment card issuers to verify cardholder identity during CNP transactions conducted via the internet. Before a transaction is authorized, a cardholder can be challenged to enter their authentication credential such as a Static Password, a Knowledge-based Response (QnA) or a One-Time Password (OTP). This additional layer of authentication has helped issuers and online merchants to counter ever-increasing CNP fraud.

Figure 1.

3-D Secure Protocol



The basic 3-D Secure solution has helped issuers substantially reduce CNP fraud, however, there are multiple challenges in the way basic 3-D Secure solutions work.

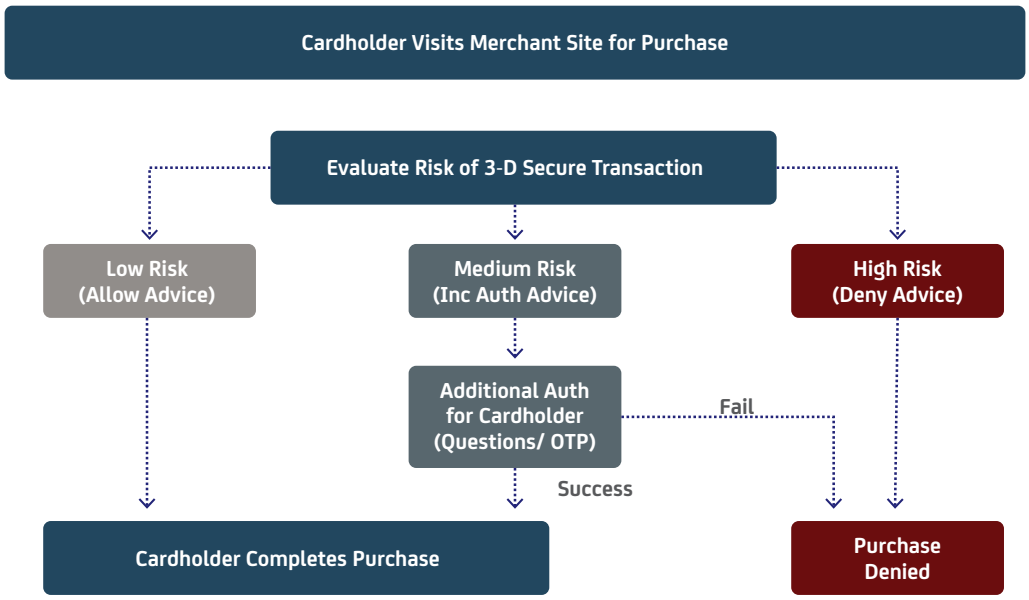
- **Optional authentication can be made mandatory** to avoid fraud at authentication, but the downside is that all cardholders, genuine and fraudulent, are challenged for authentication credentials resulting in a poor user experience and an increase in transaction abandonment.
- **Allowing users to "opt-out" and not authenticate** could provide a loophole for fraudsters by allowing them to bypass authentication during the transaction.
- **Compromised credentials could lead to "fully authenticated fraud"** where the fraudster has obtained the cardholder's credential though password cracking, phishing, social engineering or other attacks or fraudulently impersonates a cardholder and enrolls an account in 3D-Secure.

The intelligent risk analytics approach

When using only the basic 3-D Secure solution, genuine and fraudulent cardholders are subject to the same authentication challenge and user experience. This can be alleviated through the effective use of intelligence and analytics to identify legitimate cardholders allowing them to checkout without interruption. Using techniques such as device identification, merchant details, geo-location, transaction context and historical user behavior, suspicious transactions can be denied or appropriately challenged to provide stronger authentication credentials.

Figure 2.

CA Risk Analytics Outcomes



CA Risk Analytics assigns a risk score. Issuer policies use the score to separate transactions into low, medium and high risk.

By applying sophisticated risk evaluation intelligence, online shopping transactions are invisibly analyzed and assigned a risk score. Issuer policies use the score to match the type of authentication experience for the transaction. You can set your policies to provide a pleasant shopping experience for the majority of

legitimate cardholders or all premium cardholders, for example. By applying the correct follow-up mechanism for the perceived level of risk, issuers can avoid the trap of deploying "one size fits all" security measures. Figure 3 outlines the variety of risk possibilities and suggested counter measures.

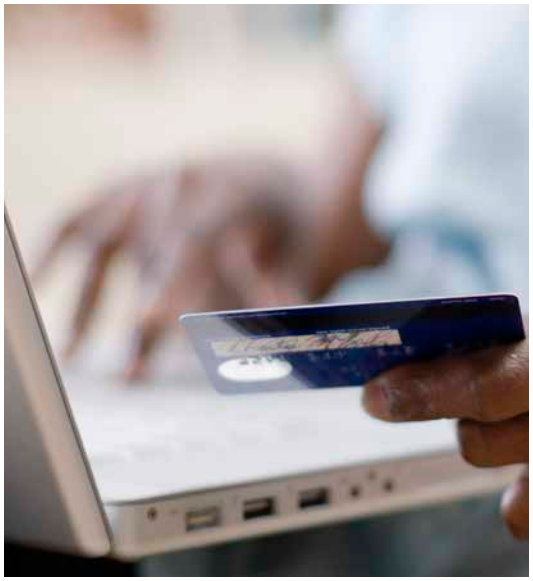
Figure 3.

CA Risk Analytics outcomes with suggested counter measures

ALLOW	**There is a high degree of confidence in the user's identity and other parameters of the requested action look to be of acceptable risk.**
ALERT	**While there is confidence in the user's identity, this request merits follow-up examination by the help desk or security team.**
INCR AUTH	**Additional confirmation in the user's identity is suggested before proceeding with request.**
DENY	**This is a high-risk transaction. Suggest that the transaction be blocked.**

Dynamic authentication for risky transactions

When additional authentication is recommended after the risk assessment, dynamic authentication can effectively validate the identity of the shopper. In the past, this took the form of a password or knowledge-based question and answer. For a higher level of security, some issuers use a one-time-password (OTP) sent via SMS. For even great security and convenience the cardholder's mobile phone can be used as an authentication device. It's important to use the most reliable form of authentication for these transactions as the goal is to take all available steps to deny the transactions that are true fraud as part of the assessment.



Cardholder behavior patterns, devices used, location and other factors can be analyzed in real time allowing the majority of legitimate transactions to continue without any change to the user experience during checkout.

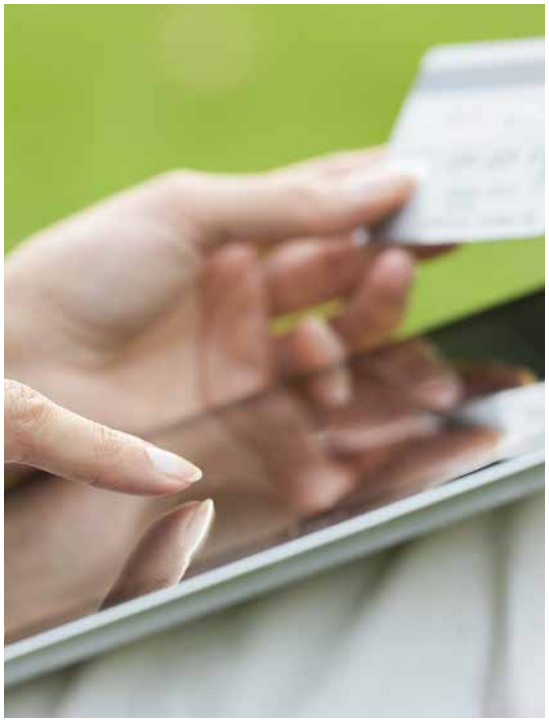
Section 2:

CA Technologies Multilayered Payment Security

Today's eCommerce landscape is expanding. In 2012, North American companies alone reported losing an average of 0.9% of total online revenue to fraud, translating to $3.5 billion[2] in fraud losses. Further, the expected adoption of EMV cards in the U.S. will improve security in card present transactions but as evidenced in the U.K., this will potentially drive more CNP fraud.[3] Throw in an 82%[2] increase in mobile commerce sales which has an even higher fraud rate than eCommerce and you have a "perfect storm" of converging fraud. How can you reduce fraud and provide security for your cardholders CNP transactions yet not deny their legitimate transactions or annoy them with requests to authenticate?

At CA Technologies, we understand the importance of reducing fraud losses while creating a friction-free customer experience. Our roots in secure digital payment technology are strong. In fact, we co-created the 3-D Secure protocol for online payment security that helped define the market. As new payment technology options have become available, we have responded with the development of sophisticated payment security solutions that help to keep fraud losses in check while providing a frictionless customer authentication experience.

Payment Security solutions from CA Technologies use a multilayered security approach to helping issuers reduce fraud and improve the online shopping experience for CNP transactions no matter where, when or on what device your cardholders use to shop.



CA Payment Security solutions use a multilayered security approach to helping issuers reduce fraud and improve the online shopping experience for CNP transactions no matter where, when or on what device your cardholders use to shop.

3-D Secure provides the foundation

CA Transaction Manager allows issuers to offer a 3-D Secure security service to cardholders. It enables full compliance with Verified by Visa, MasterCard SecureCode, JCB J/Secure, American Express SafeKey and Discover/Diners ProtectBuy cardholder authentication programs. It 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 and provides the foundation for adding advanced risk analytics to invisibly authenticate a legitimate cardholder without impact.

Key Benefits:

- Reduce fraud loss by adding an authentication layer to CNP transaction processing.
- Achieve compliance with 3-D Secure programs.
- Increase customer confidence for online shopping transactions.
- Configure business rules, security and user experience for each card portfolio.

But as noted, while reducing fraud, basic 3-D Secure impacts CNP transactions causing higher abandonment rates, lost interchange fees and higher operational costs due to chargeback processing.

Silent authentication is key

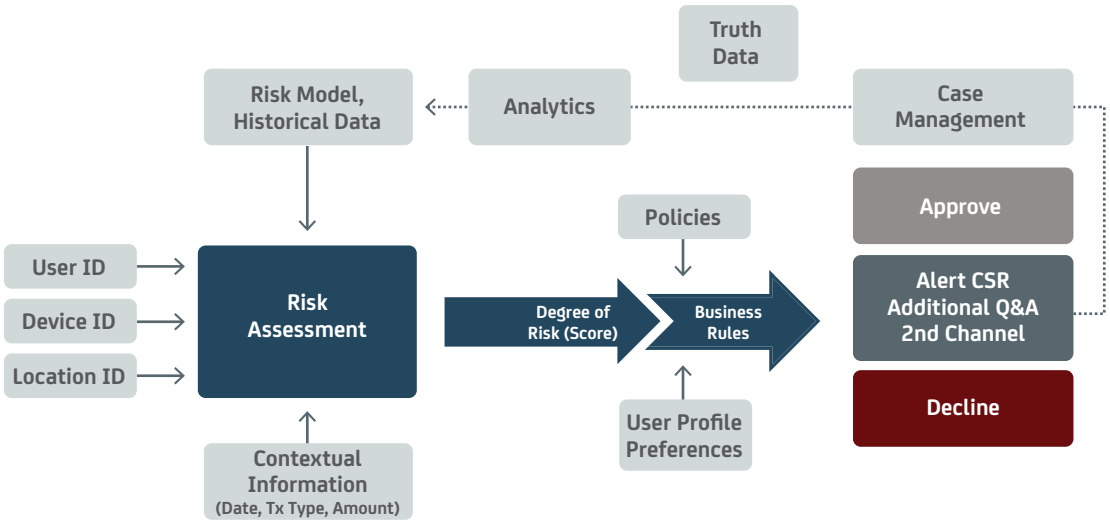
CA Risk Analytics transparently assesses the fraud risk of an eCommerce transaction in real-time during authentication. It identifies legitimate transactions allowing the majority of cardholders to continue their purchase without impact. Using sophisticated advanced analytics, a behavioral neural network model and a flexible set of dynamic rules, it examines current and past transactions, device characteristics, location, user behavior and historical fraud data to evaluate risk. The calculated risk score is then used by your policies to decide whether to allow the purchase, request step-up authentication, send an alert or deny the purchase. 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.

Key Benefits:

- Measure fraud risk in every transaction
- Reduce friction in the customer shopping experience
- Provide protection for existing payment programs
- Integrate with external fraud management systems
- Aggregate fraud data from multiple channels

Figure 4.

CA Risk Analytics work flow



Risk assessment during authentication or authorization?

Most issuers have robust risk management systems in place that are employed during the authorization phase. CA Risk Analytics does its risk assessment during the authentication phase and is meant to complement authorization systems. There is a rich set of parameters available at the time of authentication not available during authorization. Factors included in the authentication risk assessment are device identification, geo-location, and contextual information. Because there are more factors available to authenticate the cardholder, Risk Analytics during authentication has a better ability to isolate legitimate cardholders from fraudsters. Table 1 provides a comparison of factors available at authorization and authentication.

Table 1.

Parameters that are factored in risk assessment during authentication and authorization.

	Authentication	Authorization
Account Take Over Fraud		
FYP Fraud	✓	
Enrolment Fraud	✓	
Device Information		
User Machine Characteristics	✓	
Geo-location Data		
Cardholder IP address	✓	
Geo location information	✓	
Derived Data – Checks for the following:		
Negative IP List	✓	
Suspected Country	✓	
Trusted Aggregator	✓	
Zone Hopping	✓	
User Velocity	✓	
Transaction Velocity	✓	
Device Velocity	✓	
Transaction Data		
Merchant Information	✓	✓
Currency	✓	✓
Transaction Amount	✓	✓
User Specific Data		
Previous transactions	✓	✓
Risk level (designated by the issuer)	✓	✓
Authentication & Authorization Decisions		
Authentication Decision	✓	✓
Additional Authentication		
(2FA, OTP, QnA)	✓	
Ability to interact with cardholder during the transaction, e.g. IVR	✓	

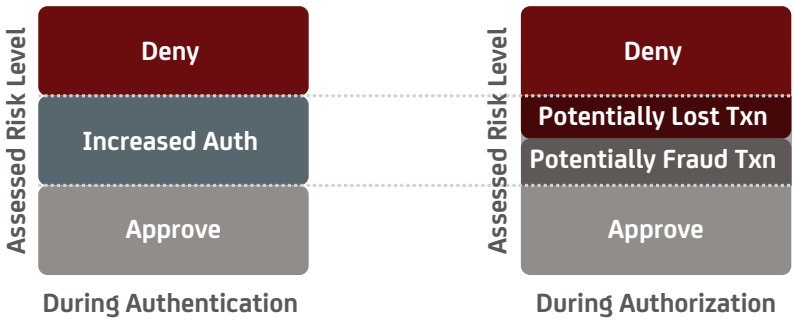


Figure 5.

Risk Assessment during authentication provides the option to require stronger authentication for suspicious transactions whereas during authorization the only choices are approve or deny.

Unlike authorization-level fraud systems that can only take binary decisions (approve or deny), CA Risk Analytics can apply increased authentication for transactions that fall in the gray area shown in Figure 5. Denying a legitimate transaction could mean lost interchange fees for the issuer and ultimately cause the cardholder to use another card.

Invoke strong authentication for suspicious transactions

CA Mobile OTP provides strong authentication using the cardholder's mobile phone as a PIN generator. Typically, an issuer sets a policy based on the risk score that allows cardholders to complete low risk transactions without impact and outright denies high-risk transactions. For medium risk transactions, the user can be challenged to provide an authentication credential. In these cases, you need a credential that provides a high level of assurance of the cardholder's identity. The CA Mobile OTP app generates a one-time password than can be entered when the cardholder is asked to authenticate.

Key Benefits:

- Easy for customer to use
- Supports variety of mobile devices
- Can be used across multiple channels

Section 3:

Why Not Get the Best of Both Worlds?

There's no question that the end goal for eCommerce transactions is to reduce fraud. More specifically, the goal is to accurately identify and accept legitimate transactions while weeding out and denying fraudulent ones. Fraud wreaks havoc on customers, merchants and issuers. Customers that have been subject to fraud may not be responsible for the fraudulent charges but certainly are inconvenienced by the hassle of following up and making sure the charges are removed from their statements. Merchants have to deal with the loss of revenue. In fact, shoppers frequently abandon an online transaction for fear that the eCommerce site is not secure. Issuers bear the burden of analyzing transactions, determining true fraud and processing chargebacks not to mention the loss of interchange fees.

Therefore, the goal of reducing fraud has to be balanced with the customer experience. Friction in the shopping experience also causes transaction abandonment and issuers need to be mindful to keep the interruption in shopping to a minimum. You don't want to deny a valued cardholder's legitimate transaction. You don't want to continually challenge your good customers with authentication requests.

The benefits of layering intelligent risk analytics on top of the basic 3-D Secure service allow issuers to get the best of both worlds: Issuers can reduce fraud losses and improve the customer shopping experience thereby reducing transaction abandonment.

Benefits of CA Risk Analytics include:

- Reduction in fraud loss over and above basic 3-D Secure deployment
- Increase in the number of transactions that are processed without customer impact
- Decrease in shopping cart abandonment
- Overall reduction in the operational costs associated with processing fraud

There's no question that the end goal for eCommerce transactions is to reduce fraud. More specifically, the goal is to accurately identify and accept legitimate transactions while weeding out and denying fraudulent ones.

Section 4:

The CA Technologies Advantage

CA Technologies has the experience and technology to help issuers reduce fraud in eCommerce transactions while maintaining a pleasant customer online shopping experience.

Experience. Our 3-D Secure solution is used by 13,000 card issuers and protects over 120 million cards. In fact, we co-wrote the 3-D Secure protocol with Visa to create an effective way to help prevent payment fraud. We've been in operation since 2000; first branded as Arcot TransFort. The cloud service is hosted from SSAE-16 Type II SOC1 audited, secure and redundant data centers. We annually certify our compliance with Payment Card Industry (PCI) data security standards and the 3-D Secure programs. Our services help you get up and running quickly.

Optimal flexibility. Offers optimal implementation flexibility to configure business rules, security features and user experience for each portfolio of cards. Multiple authentication options allow you to configure authentication by card range. Multiple administrator levels allow you to separately configure customer service agents, supervisors and administrators to meet security and compliance requirements.

Advanced Risk Models. Employs advanced models to evaluate the risk of a transaction in-flight using the amount, currency, merchant name and card identifier in combination with information that is uniquely made available during authentication including device ID, merchant URL, device IP address and information from third-party data providers. It separates fraud from non-fraud, assigns a risk score, rank-orders the score and passes it to the rules engine.

Flexible, field-programmable rules. Works in combination with the models to enforce bank policies based on the risk score. Rules bucket transactions into low, medium and high risk and action—allow, deny or authenticate—is taken based on risk tolerance. Rules can be based on transaction and session criteria and exception policies can be implemented by class of cardholder. Rules can be added or changed on the fly.

Total transparency to fraud data immediately. Allows fraud analysts to view fraud activity in real time and immediately take action to prevent fraud of a similar nature.

Real-time case management and reporting. Organizations can input "truth data" based on actual results, manage individual user profiles, and examine cases awaiting review. Using simple point and-click screens, analysts can instantly prioritize and take action on cases, query fraud data and manage alerts. An audit trail is produced that annotates each recommended action. Built-in reports provide statistical summaries and detailed case analyses.

Section 5:

Next Steps

If you're looking for a solution to CNP fraud that takes 3-D Secure to the next level, look no further. Payment Security solutions from CA Technologies provide the best of both worlds: significant fraud reduction and a frictionless customer experience for the majority of legitimate cardholders.

To learn more about Payment Security solutions from CA Technologies visit **ca.com/payment-security**. To have a salesperson contact you please email us at paymentsecurity@ca.com.

ca technologies

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

1 CyberSource 2013 Online Fraud Report

2 Based on eMarketer projections

3 Figures reported by the U.K. Payments Administration

CS200-92020_0115