ca technologies

Global Bank Achieves Significant Savings and Increased Transaction Volume with Zero-Touch Authentication

CLIENT PROFILE

Company: Global Bank
Industry: Financial Services
Geography: Worldwide
Solution: Payment Security
Products: CA Transaction Manager, CA Risk Analytics

BUSINESS

A leading provider of banking and financial services with a significant global footprint. The organization offers a range of banking products and financial services to personal, commercial and corporate and institutional customers worldwide.

CHALLENGE

Stopping fraudulent online payment transactions while delivering a smooth checkout experience for legitimate customers. Implementation needed to be quick without requiring additional internal IT resources at the bank.

SOLUTION

A secure, frictionless checkout experience for legitimate cardholders with CA Technologies "zero-touch" 3D Secure authentication solution. This first line of defense reduces card-not-present fraud using advanced models to identify legitimate transactions.

BENEFITS

The bank has detected a significantly higher number of fraud cases while impacting a smaller portion of legitimate transactions by utilizing the model scoring. This has resulted in dramatically lower abandonment rates and significantly decreased operational cost.

Challenge

Low-cost online fraud prevention that does not impact customers

The significant growth in consumers purchasing goods and services on the Internet and the increasing sophistication of on-line fraud have made it more difficult for banks to distinguish between fraudulent and genuine behavior. A shift in focus by criminals from in-store, point-of-sale (POS) fraud to online card-not-present (CNP) fraud has also been driven by the increased chip and pin security from EMV®[1] technology. With the cost of fraud detection and the volume of transactions growing, the bank wanted to ensure all its card-based services provided maximum protection.

With the above in mind, the bank's online fraud detection methods were having limited success across a range of payment card portfolios, some were particularly fraud prone.

Although important lessons had been learned over the years about consumer intolerance for multiple password authentication interfaces, the majority of the bank's card portfolios were protected utilizing a 3-D Secure™[2] (3DS) protocol requiring an additional challenge form for customer authentication on 100 percent of online transactions. The interface resulted in high shopping cart abandonment and spurred cardholders to use a different form of payment, so the bank was looking to provide a more pleasant checkout experience for legitimate customers. In addition to stopping fraudulent transactions, implementation of the solution needed to be quick and inexpensive without requiring internal bank IT resources.

The bank's card fraud mitigation team wanted to extend a high level of fraud prevention capabilities and strong customer authentication protection across their card portfolios while reducing operational cost and meeting challenging standards mandates and regulatory directives—and ultimately creating a pleasant customer experience.

With these three pillars forming the bank's challenge, the fraud mitigation team looked to CA Technologies for help in balancing effective anti-fraud efforts and a pleasant customer checkout experience for ecommerce payment transaction security.

Solution

Adaptable fraud protection unseen by the customer using the ingredients of "zero-touch" authentication

The bank turned to CA Technologies as a long-standing business partner to come up with a 3DS solution that would balance powerful anti-fraud measures with an easy customer authentication interface—and, require no internal IT support.

> "The CA account team worked with the bank to solve their need for a more advanced CNP fraud detection strategy that goes beyond simply comparing the current transaction to established fraud indicators.
>
> The obvious answer was our zero-touch authentication solution."
>
> **Nick Craig**
> Vice President of Secure Payments, CA Technologies

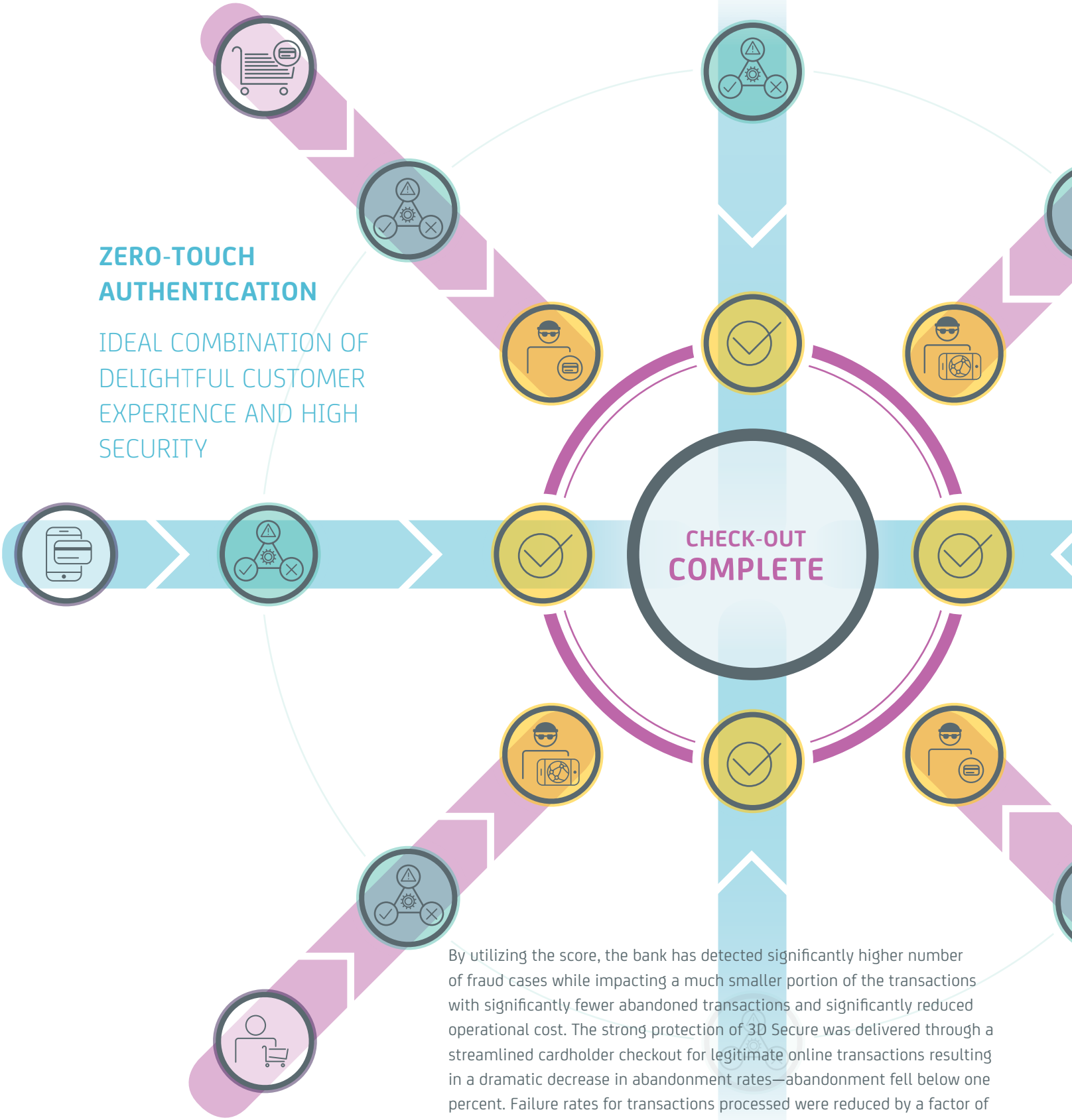
CA Technologies "zero-touch" 3DS authentication solution provides the bank a first line of defense to reduce card-not-present fraud. The SaaS-based 3DS authentication and fraud prevention capabilities are activated by CA Transaction Manager and are further enhanced by putting CA Risk Analytics into action. CA Risk Analytics is optimized for 3DS and transparently assesses transaction risk in real-time and pinpoints fraudulent actions that are occurring amidst legitimate ones with advanced neural network behavioral models, which—powered by machine learning techniques—capture data about individual user behavior.

The combination of these powerful tools authenticates legitimate cardholder transactions without interrupting the checkout process. Adaptable, dynamic rules apply business risk policies to flag suspicious transactions that require stronger authentication and produce alerts for further authentication steps or deny transactions altogether. This heightened precision in distinguishing fraudulent transactions from legitimate ones creates a secure, frictionless easy checkout experience for legitimate cardholders while helping to provide that they are protected against the threat of online card fraud. Real-time alert capability is available to the banks fraud detection team thus enabling rapid action against suspected fraudulent activity.

Thanks to the solution's fully configurable fraud prevention rules engine, the bank's fraud team can continually adapt the model thresholds as new fraud trends emerge. Rules can be adapted within a matter of minutes from the time any new threats are identified, for example from specific countries or a certain merchant. This flexibility and granularity underpin a powerful part of how the system provides the bank with greater risk management intelligence and protection.

ZERO-TOUCH AUTHENTICATION

IDEAL COMBINATION OF DELIGHTFUL CUSTOMER EXPERIENCE AND HIGH SECURITY



By utilizing the score, the bank has detected significantly higher number of fraud cases while impacting a much smaller portion of the transactions with significantly fewer abandoned transactions and significantly reduced operational cost. The strong protection of 3D Secure was delivered through a streamlined cardholder checkout for legitimate online transactions resulting in a dramatic decrease in abandonment rates—abandonment fell below one percent. Failure rates for transactions processed were reduced by a factor of sixty percent. These factors translated into the equivalent of another full-days worth of successful transactions processed successfully each month—with no increase in fraud losses.

Benefits

Fast and seamless protection against online fraud—real-time evaluation of more than 63,000 card transactions per day

As a result of the implementation of CA Transaction Manager and CA Risk Analytics, the advanced authentication capabilities give the bank greater confidence that customer transactions are secure while providing the customer with a seamless user experience.

The bank has detected a significantly higher number of fraud cases while impacting a much smaller portion of the transactions with significantly fewer abandoned transactions. Even with the increased fraud detection numbers, the bank has experienced fewer fraud cases requiring intervention and a significant reduction in operational cost. The bank realized a savings of approximately £2.6m in the first three months of implementation from just the application of CA Risk Analytics rules engine. The system evaluated more than 63,000 online transactions every day across portfolios around the world. Success was such that the bank rolled out all the tools available with CA Risk Analytics. This ideal combination includes model-based rules and a sophisticated, patent-pending neural network model that is optimized continuously by analyzing between 50 and 200 variables and over 40,000 types of data. The combination of dynamic rules and models has resulted in a reduction of fraud analyst time spent writing rules to capture edge cases and released their time to perform other data analysis activities. The bank is broadening the use of the CA Risk Analytics solution to more card portfolios.

"Risk analytics and advanced authentication models are designed to take down the fraudsters, enrich the customer experience and yield higher fraud benefit and profit."

Revathi Subramanian
Senior Vice President of Data Science at CA Technologies

Despite the solution's advanced functionality, there is no impact on the customer experience since legitimate cardholders and transactions are identified invisibly with no authentication interruption allowing approximately 88 percent of all genuine cardholders to proceed to checkout while alerting the fraud detection group at the bank to high-risk transactions in real-time thus enabling rapid action against suspected fraudulent activity.

The strong protection of 3DS is delivered through a streamlined cardholder checkout for legitimate online transactions resulting in a dramatic decrease in abandonment rates—abandonment fell to under one percent. Failure rates for transactions processed were reduced by a factor of 60 percent. These factors translated into the equivalent of another full-days worth of successful transactions processed successfully each month—with no increase in fraud losses.

CA Risk Analytics enabled the bank to protect genuine customers from fraud with minimal impact because they are not forced to enroll in 3D Secure programs, such as MasterCard® SecureCode or Verified-by-Visa®, to get the benefit of the fraud protection. The application of rules that focus on known fraud threats provide card customers with stronger protection without impacting the online experience. By decoupling the zero-touch authentication solution from IT, the bank's Card Fraud Mitigation team is better able to provide for continued operational savings by adapting to new threats and adding new portfolios.

The predictive model alone now accounts for about 70 percent of total fraud savings. Other categories in the model, such as device-blacklisting and regular rules, account for approximately 15 percent each. Before implementation, the banks authorization

model caught less than 40 percent of fraudulent transactions. Additionally, fraud data is immediately available to the bank's fraud analysts with 100 percent transparency allowing about 90 percent of transactions to be authenticated without requiring customer intervention while only the remaining transactions are challenged with stronger authentication.

Since the solution identifies a legitimate cardholder invisibly, bypassing the authentication interruption, most genuine cardholders proceeded to checkout without friction resulting in a dramatic decrease in transaction abandonment and improved the enrollment and update process. The bank has increased revenue since abandonment rates fell from four percent to under one percent.

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 EMV® technology is based on specifications outlining requirements to provide for worldwide interoperability and acceptance of secure payment transactions. Europay®, Mastercard® and VISA® (EMV) chip or "smart" cards are credit, debit or prepaid cards that have an embedded microchip, which securely stores cardholder data. For more information visit www.emvco.com.

2 CA Technologies payment security solutions provide seamless 3DS compliance with Verified by VISA®, MasterCard® SecureCode, JCB J/Secure™, American Express SafeKey® and Discover/Diners ProtectBuySM cardholder authentication programs. For more information about 3D Secure™ technology visit www.ca.com/payment-security.

CS200-141219_0715