EXECUTIVE BRIEF | JUNE 2016

Consumer Access Management for Retail

How Do I Keep My E-Commerce Applications Secure and Open for Business?

The 2016 Vend Retail Trends and Predictions Report indicates that 10 out of the 12 forecasted trends involve some form of digital transformation.[1]

The retail industry is facing major disruptions from the application economy. Everything is being driven by a connected, mobile, application-based world where your customers are far more likely to experience your brand and interact with your enterprise through a software application rather than a live person. To thrive in this new reality, retail organizations need to make digital transformation and a superior user experience their top priorities.

Today, digital is everywhere—big data, cloud, mobile, social and the Internet of Things are changing the way we all work and play. Digital business is the future for successful retailers, and delivering the same level of support and service online that customers receive from traditional brick-and-mortar stores is the ultimate goal. But three major challenges are standing in retailers' way:

- **Omnichannel**. Mobile applications are undoubtedly the next wave in the evolution of e-business. In fact, they've become the strategic initiative for all digital organizations looking to drive business forward. Yet retailers struggle with delivering the same user experience across all online channels, and a poor user experience can directly result in lost revenue.
- **Shopping cart abandonment**. Retailers continue to experience high abandonment rates for their e-commerce applications as potential buyers fail to complete their purchases. Reducing friction and increasing customer loyalty could help convert some of these abandoned shopping carts, which would result in increased revenue.
- **Online identity fraud**. Although most people associate online fraud with credit-card theft, criminals have found new ways to commit fraud and loyalty programs are one of the latest targets. As a result, more-effective authentication mechanisms are rapidly becoming a necessity for consumer-based Web sites and mobile applications.

Omnichannel

70 percent of the world's population will use smart-phones by 2020.[2]

As mobile commerce continues to gain momentum as a mainstream way for consumers to shop online, retailers are heavily investing in creating user-friendly, feature-rich mobile applications as a core part of their digital transformations. Reaching customers through these growing channels and keeping them satisfied with amazing experiences will become a default practice for any successful business.

With the emphasis on transformation, omnichannel or digitally connected multichannel capabilities, have become a key focus area. The ultimate goal is to deliver a branded, consistent, integrated and holistic customer experience. The challenge comes in balancing the need to craft a uniform experience while simultaneously developing a unique, customized flow for the individual customer.

This means that software development organizations are under increased pressure to deliver a new generation of software apps—and the application programming interfaces (APIs) required by external partners to build an ecosystem of value around the connected product. This has created the need for a digital transformation strategy as an organization shifts how it uses technology from being a cost center and operational function to a genuine competitive differentiator.

63 percent of users will access online content via their mobile devices by 2017.[3]

From a purely technical perspective, designing an API is relatively easy, but designing one that contributes real value to the business can complicate matters. Beyond functionality, enterprise architects must also consider business goals and the end-user experience.

As well as opening up a world of business opportunities, APIs have the potential to open the enterprise to serious new security threats by exposing sensitive back-end systems and data to the outside world. APIs are vulnerable to many of the security threats that have plagued the Web, plus a range of new API-specific threats. Therefore, it is vital to deploy strong, API-specific security at the edge of your API architecture.

The most efficient way to create a centralized and secure API architecture is to deploy an API management solution. In addition, in order to avoid a new security silo and leverage the same security policies and contextual risk analysis across all channels, the organization needs to integrate its API management solution with its Web access management solution.

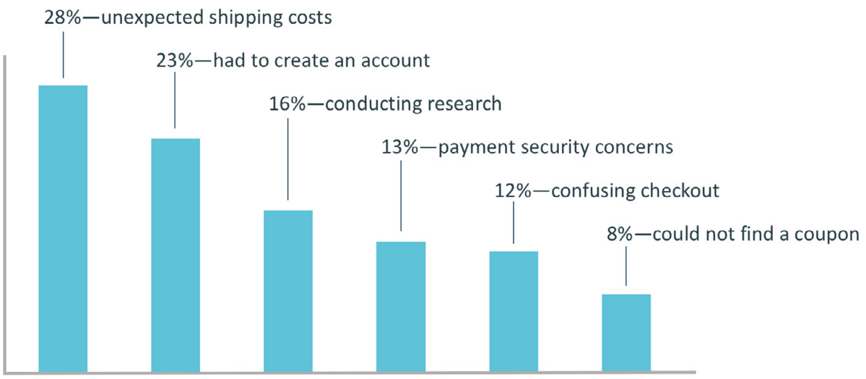
Building an infrastructure that centralizes common architectural components of secure, developer-centric APIs can significantly simplify the process of implementing APIs that add real value to your business.

Shopping Cart Abandonment

The rapidly evolving digital world is redefining the relationship between your business and your customers, who now expect a convenient, frictionless, interactive and secure experience from their shopping transaction. And as retailers make significant investments in creating user-friendly websites and mobile applications, they face yet another obstacle—shopping cart abandonment.

Figure A.

Top Causes for Shopping Cart Abandonment[4]



The average shopping cart abandonment rate in 2015 was approximately 68%, and the estimated value of these abandoned carts was approximately $4.9 trillion.[5]

The omnichannel access solution from CA Technologies addresses two issues associated with shopping cart abandonment:

- **Required account creation**. Users don't want to be forced to create a new account and a new password for every site they visit. Using social media credentials can eliminate or significantly reduce the time required to create an account, which could reduce the number of shopping carts that are abandoned for this reason.
- **Payment security concerns**. Consumers want to know that their personal and financial data is secure. By increasing the authentication required to access a user's account and make purchases, the retailer can enhance customer loyalty and retention, which could result in more positive reviews and social commentary—thereby attracting new customers.

Online Identity Fraud

Not surprisingly, online identity fraud and data breaches remain at the top of the list of retail concerns. Security is a critical part of any kind of digital transformation initiative, and the stakes are high. Cybercriminals have expanded their reach beyond traditional targets of consumer banking and credit cards—focusing now on other forms of online fraud and harvesting sensitive personally identifiable information (PII) and protected health information (PHI) data that is being exposed online.

According to the recent Symantec Internet Threat Report, Retail is the third most breached sector—with almost 10 percent of the reported cases.[6]

In the past two years, we've seen a wave of attacks aimed at loyalty programs. United and American, Hilton and British Airways all announced breaches to their loyalty programs.[8] In each case, hackers stole the users' credentials and then logged in and impersonated the user to purchase gifts, airline tickets and hotel rooms. More recently, Kohl's experienced a similar breach;[9] however, in this case, the hackers purchased expensive items, shipped them to the legitimate user's home address, then cashed in the loyalty points before the goods could be returned.

Loyalty program breaches not only result in financial losses for the business; they also may result in lost customers—the opposite of what a loyalty program is intended to do. According to a recent study,[10] 85 percent of respondents claimed they would take their business elsewhere if their favorite retailer experienced a data breach.

In 2015, 95 percent of Web application breach incidents that Verizon investigated involved hackers impersonating users with stolen login credentials.[7]

As retailers address the security of their e-commerce and loyalty program sites and apps, they can look to the payment card industry for best practices and lessons learned in combating online identity fraud. The credit card industry has long been a target for fraud and has deployed an array of technologies to fight it, especially for online purchases. However, organizations also learned that increased security can also lead to transaction abandonment and lost revenue when they introduce too much friction into the process.

To address that friction problem, the credit card industry discovered that combining risk analytics and user behavioral profiling with the authentication and authorization process could significantly reduce the abandonment rate. One credit card issuer found that adding CA Risk Analytics to its 3D Secure solution, CA Transaction Manager, reduced the abandonment rate to under one percent and saved more than $3 million dollars in the first three months of implementation.

Implement your digital transformation initiatives without sacrificing security or customer experience.

To take full advantage of the e-commerce opportunity, retailers must open up their traditional boundaries and connect valuable and sensitive data to the outside world. It's what today's consumers expect and what app-based competitors are already doing.

From home, the office or on the road, people want the convenience of being able to buy goods and services, make reservations, book travel and share experiences with social networks. While retailers work feverishly to meet the demand, they need to be aware of the extreme security threat involved in enabling these digital transformation initiatives.

Retailers need a more comprehensive strategy—one that not only simplifies the access management experience for consumers and business partners but ensures privacy and protection of sensitive data. CA refers to this as omnichannel access, and has developed a solution that delivers four key capabilities:

Social registration. When users can leverage their existing social media identities (from sites like Facebook, Twitter and Google+) to log into your site or portal, it streamlines the login process and gives them one less password to remember. While social logins reduce friction, they can pose a security risk, so it's important to have step-up authorization processes in place when more sensitive transactions are being attempted.

SSO and federation. If you can provide seamless access for customers and partners to your mobile or Web applications, portals and security domains via a single sign-on, it makes it easier for them to consume more of what you offer, which helps strengthen your relationships and open up new, or bolster existing, revenue streams.

API management. Digital initiatives based on APIs are all about providing scalable, reliable connectivity between data, people, apps and devices. If you can solve the challenge of integrating systems, adapting services, orchestrating data and rapidly creating modern, enterprise-grade APIs from different sources, then you can significantly accelerate your digital transformation.

Context-sensitive security. Whether users authenticate with social media credentials or log in directly with a password, both leverage credentials that are inherently insecure and can easily be stolen. It's critical to apply risk analysis and user behavior profiling to the authentication process so you can more accurately identify legitimate users and issue an out-of-band, step-up authentication challenge when the context of access appears too risky.

Today, an app's UX has come to embody the characteristics of a product or service that are important to the individual. It's the recognized feeling one receives when interacting with your brand and the lasting memory the individual has after connecting with your business. This influences their loyalty and willingness to recommend your brand to others in their social network.

The ability to engage and accomplish tasks in a minimal amount of clicks has changed the mindset from show me everything I could do, to show me only what I need to do. Consumers want a frictionless experience. While security isn't the only thing that inhibits a good experience, it plays an important role. The problem with security as it's typically deployed is that it can negatively impact the UX and hinder adoption and customer loyalty. The omnichannel access solution from CA addresses this area by providing a more secure way to protect against online identity fraud and ensure data privacy without undue burden for the customer.

For more information, please visit **ca.com/security**

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] Vend, "2016 Retail Trends & Predictions"

[2] Ericsson, "Ericsson Mobility Report," June 2015

[3] Statista, "Facts on Mobile Internet Usage," 2015

[4] Click Z, "Why Do Customers Abandon Online Shopping Carts," November 19, 2015

[5] Baymard Institute, "33 Cart Abandonment Rate Statistics," January 14, 2016

[6] Symantec, "2016 Internet Security Threat Report," April 2016

[7] Verizon, "2015 Data Breach Investigations Report," March 2015

[8] Robert Marti, "Online Identity Fraud: It's not just about credit cards," CA Highlight blog, April 20, 2016

[9] Brian Krebs, "Fraudsters Tap Kohl's Cash for Cold Cash," Krebs On Security, February 2016

[10] Vormetric, "2015 Insider Threat Report," 2015