Aligning payment security to your digital business transformation strategy

FIVE KEY CONSIDERATIONS:
FIVE KEY CONSIDERATIONS:
Aligning payment security to your digital business transformation strategy

Throughout the last decades of the 20th century and into the 21st, innovation around core banking objectives has been steady. The evolution of cash, checks and credit cards changed the way consumers thought of banks, and changed the role banks played—even as they remained at the center of financial thinking. Innovation in payments, meanwhile, was relatively static.

But in the last decade, innovation in the payments world has caught up quickly. The advent of commerce on the internet led disruptive technology providers—who began to espouse disintermediation as a fundamental good—into payment providers. Adapting to a digital world led those disruptors to create digital services that seemed to put banks at a disadvantage in a world that moved at light speed.

While banks have not traditionally figured payments into their broader objectives, they responded by beginning to see payments as integral to engaging clients, and building loyalty and brand trust in a digital environment. To meet customer demands to engage with the digital economy, banks realize that they must transform to provide payments and other digital services that are faster, more convenient—and most important—more secure than ever before. Which is why banks must consider payment security as part of their institution’s broader digital strategy.

This document provides specific recommendations designed to help banks align payment security and support a comprehensive digital business transformation strategy.

Innovation in Financial Services

More than making it easier to catch a ride, watch episodes of your favorite TV show or buy a Christmas gift from your couch, the sharing economy has made payments seamless. Services like Uber, Netflix and Amazon are now part of the fabric of our lives, and all indications are that financial services are the next frontier where digital services will usher in a wave of innovation. But banks that want to ride that wave must contend with an unfamiliar competitive landscape and, from a risk-management perspective, an increasingly sophisticated threat environment.
Because consumers are accustomed to the various digital services that make their lives easier, they're more than willing to look outside the traditional banking world for financial services. A recent survey of 4,000 consumers in Canada and the U.S. reveals that 11 percent of consumers switched financial services providers in the past year, including to virtual banks.¹

FIGURE 2. Online-virtual banks followed by payments providers lead in net switching among consumers who switched.

Q: In the past 12 months, have you switched to a new financial services provider or other company from your main bank?

<table>
<thead>
<tr>
<th>Financial Service Provider</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online-Virtual Bank</td>
<td>11%</td>
</tr>
<tr>
<td>Payments Provider</td>
<td>3%</td>
</tr>
<tr>
<td>Local Community Bank</td>
<td>1%</td>
</tr>
<tr>
<td>Credit Union</td>
<td>1%</td>
</tr>
<tr>
<td>Insurance Company</td>
<td>0%</td>
</tr>
<tr>
<td>Brokerage-Wealth Manager-Financial Adviser</td>
<td>0%</td>
</tr>
<tr>
<td>Retailer</td>
<td>-1%</td>
</tr>
<tr>
<td>Online Lender</td>
<td>-2%</td>
</tr>
<tr>
<td>Large Regional or National Bank</td>
<td>-15%</td>
</tr>
</tbody>
</table>

These numbers represent even more proof that meeting consumer demands is more important than ever. And, banks will have to keep customers happy in a global environment where the combination of an inexorable rise in online transactions and the U.S. EMV migration will cause a significant jump in the number and sophistication of fraud attacks worldwide.
FIVE KEY CONSIDERATIONS:
Aligning payment security to your digital business transformation strategy

The Role of Payments

If banks must indeed undergo a digital transformation to remain competitive, they should leverage payments to achieve that goal. A reduction in the number of bank branches is one indication that a move toward offering digital services is already underway. But payments—which are increasingly mobile, wallet-based and frictionless—are one way to provide consumers with the experiences they expect. For issuers, it’s paramount to let customers add their cards to their preferred digital wallets.

Digital Business Transformation

We’re in an age where technology and innovation are changing the world for the better. Banks that want to drive customer loyalty and business performance by making customers’ financial lives easier and more convenient must commit to broad-based digital business transformation. This requires attention and change throughout the entire business—not only to back-end technology but by committing to the customer experience and viewing IT and security in ways that transcend cost.

The components of a digital business transformation will vary depending on the type of financial institution or provider in question. All business, however, must align such a change to a top-down strategy that embraces technology as a business enabler and is committed to being agile.

An agile bank or processor transforming itself to serve its customers should position its digital architecture in a way that optimizes the back end—people, processes and compliance—and focuses on fulfilling customer needs to drive growth. These include payments, digital banking and an entire omnichannel experience that integrates physical branches.
FIVE KEY CONSIDERATIONS:
Aligning payment security to your
digital business transformation strategy

Organizations will need to be prepared for challenges that can derail a move toward
digital, including competitive disruption (from banks and non-banks), new security threats,
operational costs or even a lack of prioritization. But, companies that emphasize the
following best practices will be able to navigate the transition more smoothly.

The Five Key Considerations

1. **Embrace APIs.** The most important shift necessary to ensure the success of a digital
   business transformation is to champion the use of application programming interfaces
   (APIs). APIs are the mechanism by which you will connect your service to the rich, third-party
   features that provide the design and user experience that consumers demand. Take Uber for
   example: the company uses APIs to integrate maps and payment—the two characteristics
   that are the essence of the experience—into the app. APIs will be critical to delivering the
   level of service your customers expect. And because they connect your service with a third
   party, API management and close oversight of security are critical.

2. **Utilize Big Data analytics efficiently.** An organization undergoing a digital transformation
   will produce enormous amounts of data, and using computing power to extract meaningful
   intelligence from that information is crucial. For issuers, leveraging that information to
   authenticate users during payment transactions or when accessing online accounts, for
   example, would positively impact and tremendously improve the customer experience. One
   global bank that implemented a zero-touch authentication solution from CA saved $3.2
   million in three months, and dramatically reduced abandonment rates. CA’s zero-touch
   authentication uses big data analytics to evaluate risk during card-not-present transactions.
   It accurately identifies genuine customers to let those transactions proceed, and only
   prompts additional authentication steps for risky transactions.

3. **Embrace agile principles to manage outcomes, not outputs.**

4. **Unite development, operations and product teams.**

5. **Redefine security as a business enabler.**
FIVE KEY CONSIDERATIONS:
Aligning payment security to your
digital business transformation strategy

3. Embrace agile principles to manage outcomes, not outputs.
From a software development perspective, the emphasis shifts from outputs like KPIs and time-to-delivery toward outcomes that effect customers, like time-to-value, abandonment rate and customer satisfaction.

4. Unite development, operations and product teams. Typically, launching an app requires significant coordination between development and operations. When those teams aren’t aligned, delivery time, quality and security can all suffer. With a combined DevOps strategy, organizations can develop and launch far more efficiently.

5. Redefine security as a business enabler. In the banking and payments world, security has been seen as the brake pedal when it should really be considered the engine. How companies can use data has transformed the way they think about security. In its first incarnation, 3-D Secure saw its fair share of criticism by merchants and processors, especially in the U.S., because it asked all users to authenticate themselves with an extra password—a step that negatively impacted conversions and abandonment rates.

New data analysis techniques have enabled a risk-based approach to 3-D Secure that has rendered it invisible to legitimate customers. Thus, a security measure using a predictive model to identify legitimate customers reduced the number of users who abandoned transactions to less than one percent, enabling incremental business.

Embracing Agile: In 1954, the famous business consultant and author Peter Drucker wrote about the philosophy a business must have if it is to be agile and thus, able to reinvent itself when it struggles. In “The Practice of Management,” he urged organizations to remember that a business is not the physical plant, the processes, the employees or even the product. A business is only the value created for a customer. Agile organizations keep a relentless focus on the customer and a digital business transformation must be focused first on delivering value that matters to customers and then on leveraging technology to make that happen.

EMVCo Announces 3-D Secure 2.0:
EMVCo, the body that manages security specifications for chip-based payment cards, recently announced several advancements to the 3-D Secure protocol. For instance, EMV 3-D Secure 2.0 will request richer cardholder and device data during the transaction, resulting in far fewer password interruptions. As a leading provider of 3-D Secure solutions, CA Technologies is the ideal partner to help issuers migrate to EMV 3DS 2.0. Our payment solutions support existing 3-D Secure protocols and help issuers prepare for EMV 3DS 2.0, enabling them to easily accept transactions from all merchants. To get ready for EMV 3DS 2.0, issuers should work toward a consistent customer journey, adopt an analytics-driven approach to risk-based authentication and adopt one-time password methods for stronger authentication.
Payments and Security as Part of Digital Business Transformation

When a digital business transition has been achieved, recognizing a shift in customer needs should naturally follow. In the case of banks and payments, agile issuers understand that their customers live in a new reality that includes innovators of all stripes offering them financial services. Most already see the link between payments and the bank’s broader objectives. But executing on a payments strategy will likely require more collaboration with FinTech companies that may have previously been considered adversaries. True transformation is challenging, but agile management and intelligently leveraging technology while protecting customers with frictionless security will enable committed organizations to reach this goal.

For more information on Digital Business Transformation, tune in to our on-demand webcast: Reality Check for Digital Wallet Security
FIVE KEY CONSIDERATIONS:
Aligning payment security to your
digital business transformation strategy

About CA Technologies
CA Technologies is a leader in securing 3-D Secure card-not-present transactions, protecting over 200 million cards worldwide. Our Payment Security solutions provide zero-touch authentication helping card issuers minimize online fraud while providing a frictionless checkout experience for cardholders. Sophisticated risk analytics and dynamic, granular bank-defined rules help to identify emerging fraud patterns and take action on potentially fraudulent transactions in real time. In addition, the advanced neural network models analyze available data to accurately identify legitimate transactions reducing the number of genuine transactions that are declined. Our case management system provides immediate access to fraud data to help manage fraud alerts and cases more efficiently. As a result, issuers can more effectively combat eCommerce fraud, decrease transaction abandonment and create a better experience for cardholders. To learn more about our Payment Security portfolio, please visit www.ca.com/payment-security.

About CardNotPresent.com
CardNotPresent.com, part of the RELX Group, is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. The company’s media platforms include the CardNotPresent.com portal, the hub for news, information and analysis about the payments issues that most affect merchants operating in the space; the CNP Report, an e-newsletter delivering that focused information directly to your email inbox twice a week with no extraneous clutter; the CNP Expo, an annual gathering of the leading companies in the space from the smallest e-commerce Websites and technology providers to global retailers and payment processors; and the CNP Awards, an annual event honoring the products and solutions CNP merchants rely on most to increase sales. For more information, visit www.CardNotPresent.com.

This document was produced as a joint effort between CardNotpresent.com and CA Technologies.

FOOTNOTES