opusresearch »

Stop the World! I Need to Get Auth

How Financial Services Companies Can Offer Seamless Secure Messaging

By Dan Miller | Lead Analyst & Founder, Opus Research | May 2019

Banks, insurance companies and investment houses don't really want to stop the world from moving; however they have to acknowledge that messaging-based commerce often comes to a complete stop when one of their clients has to pivot from a public platform - like WhatsApp, Facebook Messenger, WeChat, Line or Twitter – to their secure Web site or mobile app. While many messaging apps purport to be secure by incorporating end-to-end encryption and relatively strong authentication methods, those forms of security deal with individual privacy and protection of personal data while on a single platform.

When an individual wants to transfer funds, change an address or send credit card information to make a payment, things fall apart.

Security and privacy have, rightfully, taken center stage as billions of people around the world turn to chat channels and messaging platforms to carry out both communications and commerce. Look no further than your TV to see how Apple has made privacy central to an advertising campaign that started with billboards at the Consumer Electronics Show in Las Vegas and culminated (so far) with 30-second spots at crunch time - some of the most highly-viewed segments of March Madness (the U.S. Men's College Basketball playoffs).

In spite of the history of sharing-to-the-point-of-oversharing, users of the most popular messaging platforms still have an expectation of privacy, or at least of control over what they reveal about themselves to banks, brands and the rest of the world. As focus turns to Conversational Commerce, and the role of messaging in forging bonds between companies and their customers, use cases call for strong authentication, end-to-end encryption and compliance with both laws and financial industry regulations designed to prevent fraud, protect privacy, and promote security. As the industry is concocting new use cases, we're witnessing the classic balancing act between security and convenience.

From a technology perspective, secure messaging starts with end-to-end encryption and strong assertions that the individual who initiates a messaging thread and eventual transaction is indeed whom they claim to be. The problem of strong, continuous authentication is made more complicated because conversational commerce is often asynchronous, meaning that it takes place over a period of time, using multiple platforms. Avid messaging platform users are agile. When shopping, they start with search. Then they consult with friends or trusted advisors. When it comes to dealing with a specific brand, they will transfer or "pivot" from one of the public platforms mentioned above into a company's secure, branded website.

Well, Good-bye to All That

Apple, Sparkcentral, and others are taking approaches that make the transition from routine daily messaging to secure conversational commerce seamless from the point of view of the end-user. Similar to shopping on the public Web, when the customer indicates that she is ready to make a purchase or complete a transaction, she is informed that she is "leaving" the chat-based conversation on Facebook Messenger or SMS and logging on to a secure chat channel with the brand, often a webview inside the messaging app, realized through the use of a redirected or embedded HTTPS link.

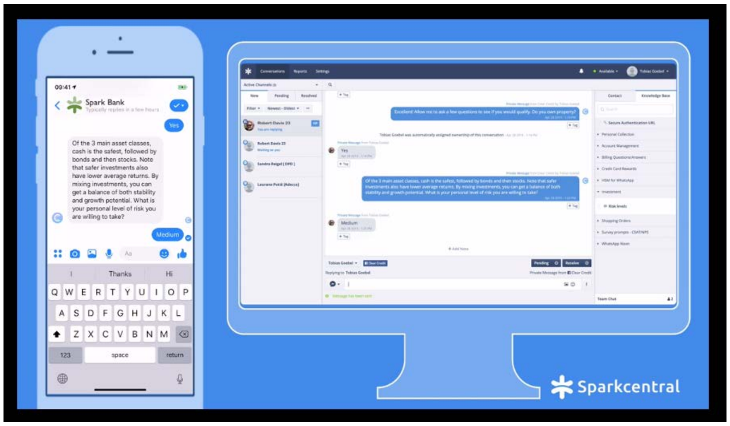
The pivot takes place in a way that not only promotes confidence on the part of the shopper – the "lock icon" in the browser's navigation strip can do that – but also supports assertion of identity, authentication and log-on with the click of a button or link in the course of the conversation. Meanwhile, the collection of sensitive data such as credit card numbers is performed in the secure Web outlet, never exposing it to the messaging provider or anyone else.

Here's a Case in Point

Recognizing that messaging use is on the upswing while visits to brick-and-mortar branches are in steady decline, banks and financial services companies are taking secure messaging seriously. In this respect we're seeing a pronounced shift in their security and fraud departments from "No way! No how!" to "Here's how we can effortlessly log a messaging user onto our secure site."

Have a look at this case study from Sparkcentral a messaging customer service platform provider that focuses on connecting companies to their customers through multiple messaging channels.

In the video, a client of Spark Bank, Robert, starts a conversation with a financial advisor on Facebook Messenger with the intention of investing in a mutual fund. The advisor determines that the conversation must conclude on a secure channel and invites the client to pivot to the mobile app.



09:41

Spark Bank

Yes

Of the 3 main asset classes, cash is the safest, followed by bonds and then stocks. Note that safer investments also have lower average returns. By mixing investments, you can get a balance of both stability and growth potential. What is your personal level of risk you are willing to take?

Medium

https://info.sparkcentral.com/secure-messaging-demo

The link sent by the advisor renders itself as a convenient button in Messenger. Once in the bank's secure mobile app, the chat history is preserved and both the client and the advisor can conclude the transaction.

What is impressive to note is that the log-in and authentication has taken place in the background, to the satisfaction of the bank and without any effort from the client.

A True Pivot for Secure Messaging

In the past, banking clients on messaging platforms could only go so far before they made individuals jump through hoops or flaming hoops devised by security professionals. Waiting for one-time-passwords to be delivered via text message or struggling to remember the answer to "challenge questions" that, in many cases were manufactured from "in wallet" data. (Quick, do you remember the exact amount of your last credit card purchase). To support a client's ability to pivot from one channel (Facebook Messenger) to a more secure channel offered by the bank, be it a Webview or secure messaging in the bank's app, a provider like Sparkcentral must step in to provide an authorization code or "token" that asserts to the bank that Robert is who he claims to be and links his messages to the new secure conversation.

On the bank's secure link, the authenticated Robert can carry on conversations that culminate in transactions, even provide credit card numbers or other personal information with the confidence that his data is safe from bad actors.

As the use cases provided here demonstrate, once a user successfully logs onto their messaging platform of choice, mechanisms exist that enable banks to accept their credentials with confidence. Little or no extra effort is required. Opus Research calls it Intelligent Authentication. Messaging-centric platform providers like Sparkcentral and its partners make it a reality.