

B2B PAYMENTS

Signature Bank Launches Blockchain Real-Time Payments For Corporates

By PYMNTS  

Posted on December 5, 2018

 SHARE TWEET SHARE SHARE PRINT EMAIL

New York-based Signature Bank is rolling out a digital payments platform powered by blockchain that enables real-time payments for corporate customers.

The financial institution **announced** on Tuesday (Dec. 4) the launch of its payments platform, Signet, to provide digital payment services for corporate customers. The platform was developed in partnership with **blockchain** company trueDigital Holdings, Signature noted, and will go live on Jan. 1, 2019.

“Signet will quickly prove to be extremely beneficial and revolutionary for our commercial clients, as they will now be afforded the opportunity to make instantaneous USD payments to one another in real-time (24x7x365) at no cost per transaction,” said the bank’s Chairman of the Board Scott A. Shay in a statement.

Shay pointed to use cases for **commercial real-time payments**, including within the “wholesale energy distribution market and over-the-counter institutional trade and settlement activities.”

The solution enables corporate payments made in real time at any time throughout the year without transaction fees. Companies must have a minimum of \$250,000 in their accounts to conduct payments using the platform.

In its announcement, Signature noted that rather than funds requiring the intervention of two different financial institutions to move money between two parties, the platform enables funds to be moved in real time between corporate customers, as long as both are clients of Signature Bank.

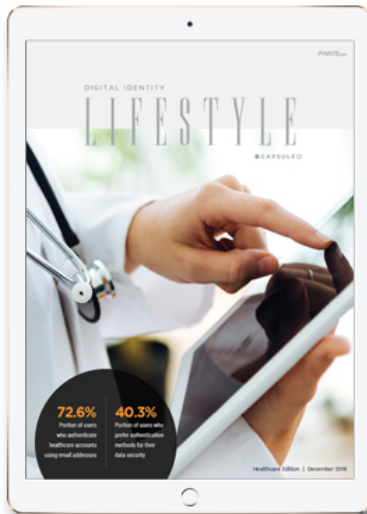
The bank said the New York State Department of Financial Services has provided approval for the platform, and deposits held within Signet are eligible for **FDIC** insurance.

In a statement, Signature Bank President and Chief Executive Officer Joseph J. DePaolo said the ability for corporates to make real-time B2B payments is “very valuable, especially in light of the increasing speed and frequency at which they conduct their business.”

He noted the support of the state’s Superintendent Maria Vullo and the Department of Financial Services, which, he added, have “thoroughly researched the financial technology arena and understand how it impacts the future of financial services.”

LATEST INSIGHTS:

Our data and analytics team has developed a number of creative methodologies and frameworks that measure and benchmark the innovation that’s reshaping the payments and commerce ecosystem. **Check out the latest PYMNTS report on healthcare digital identity.**



DOWNLOAD NOW



PYMNTS.com

DIGITAL IDENTITY LIFESTYLE CAPSULE 2018 HEALTHCARE EDITION

RELATED ITEMS: B2B, B2B PAYMENTS, BLOCKCHAIN, COMMERCIAL BANK, CORPORATE BANKING, DIGITAL PAYMENTS, NEWS, REAL TIME PAYMENTS, WHAT'S HOT IN B2B

SHARE

TWEET

SHARE

SHARE

PRINT

EMAIL

B2B PAYMENTS

The Security Threat Of Bank-FinTech Collaboration

By PYMNTS

Posted on December 5, 2018

[f SHARE](#)[TWEET](#)[in SHARE](#)[SHARE](#)[PRINT](#)[EMAIL](#)

When the data of 15 million **T-Mobile** customers was stolen in 2015, the mobile firm's CEO immediately went into damage control mode. John Legere released a **statement** when the news broke, offering customers access to free credit monitoring and identity resolution services, and emphasizing the company's efforts to assist clients concerned about their privacy.

Here's the kicker: It wasn't T-Mobile's fault. Rather, a hack at its credit reporting vendor **Experian** led to the data breach. Even so, the damage had been done. T-Mobile executives had to allocate time and resources to protecting the brand. In addition, while the communications company was not held liable (and wasn't the target of a subsequent **class action** lawsuit), T-Mobile almost certainly lost some confidence among customers, with headlines using the T-Mobile name — not Experian — to relay the news.

"It wasn't really their fault, but that doesn't matter," explained Jonathan Simkins, chief financial officer of cybersecurity firm **CyberGRX**, to PYMNTS in a recent interview, reflecting on the repetitional damage that T-Mobile incurred. "Your average customer trying to buy a cell phone doesn't understand any of that — and has no interest in understanding it."

The case highlighted the threat of third-party cyber events, which are rising in frequency, according to the **Ponemon Institute**. The firm released its “Data Risk in the Third-Party Ecosystem” study last month, and found that 59 percent of more than 1,000 executives surveyed said they had experienced a data breach as a direct result of a cyberattack on a vendor or other **third-party** partner.

The research was published the same month in which another third-party cyber incident nabbed headlines. Hospital network **Atrium Health** revealed that the data of up to 2.65 million patients may have been exposed, all thanks to a **data breach** at one of its vendors, healthcare technology provider **AccuDoc Solutions**.

Risk mitigation isn’t a new concept, Simkins noted, but today’s organizations are often unfamiliar with the correct strategies they need to deploy when mitigating third-party cyber risk. While this threat affects companies of all industries and sizes, large multinational organizations — with thousands of vendors and third-party partners — can struggle the most.

“I would characterize it as a Big Data issue — it’s very intimidating to get started in third-party risk management,” Simkins said. “It gives you heartburn, all the work you have ahead.”

Inexperienced or unfamiliar professionals may take a bottom-up approach to third-party risk management, analyzing risk on a vendor-by-vendor basis. A company with 10,000 suppliers, however, won’t get far without spending years on this tactic. According to Simkins, organizations must deploy the right cybersecurity products and strategies to identify the highest-risk vendors first, and work from there.

With the threat of third-party cyber risks rising, the financial services (FinServ) industry is especially prone to hacks that can ripple through supply chains. This is particularly true as open banking initiatives encourage bank collaboration with third-party FinTech firms and facilitate the movement of data between platforms. Now, financial services players have access to more customer data than ever before.

“Banks liked to do things in-house, [but] that attitude has been changing for the last decade — they’re much more willing to partner with what’s not really a financial services company, but a tech startup to help them outsource product development and stay competitive,” Simkins said.

While this benefits the business development, strategy and revenue-generating sides of a 100-year-old bank (not to mention, supports growth in market share, much to the pleasure of shareholders), the trend puts significant pressure on the risk management side of a financial institution (FI). Banks are often applying decades-old risk management strategies to their cyber risk management efforts, according to Simkins, because they lack the adequate understanding and experience of cybersecurity, as well as third-party risk management on a cyber level.

“They manage credit risk and liquidity risk, and more traditional third-party risk verticals,” he said. “They know how to do it, and are very comfortable with it. But the cyber risk is new.”

If one thing has emerged as a universal truth in cybersecurity, in the wake of numerous high-profile attacks and data breaches, it’s that the threat of a cyberattack can never be completely eradicated — at least, not today. However, organizations must do as much as they can to safeguard their systems, prevent as many attacks as possible and figure out how to bounce back from an incident should it occur. Increasingly, this includes addressing third-party risks in firms’ cybersecurity strategies, and cybersecurity service providers like CyberGRX are stepping in to fill knowledge and experience gaps.

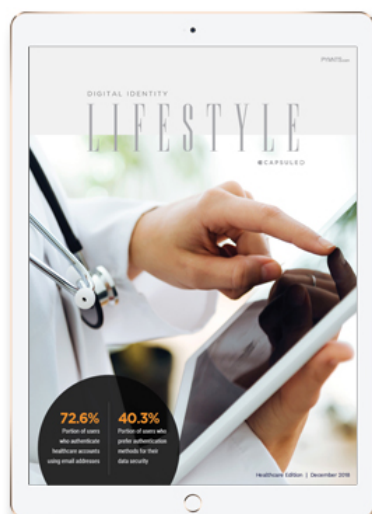
Last week, the company **announced** a \$30 million fundraise as it works to address this issue. The Series C funding was led by Scale Venture Partners, while Aetna Ventures, Bessemer Venture Partners and other backers also participated in a show of support for third-party risk mitigation technology.

Unfortunately, because this area of security and risk mitigation is relatively new, especially for legacy FIs, Simkins said there is still much that security experts have to figure out.

“It’s not brand new,” he said, “but it’s new enough that you don’t have a guy at the bank who’s been doing this for 30 years, who’s awesome at it and can [teach] the rest of the enterprise. Everyone is trying to figure it out on the fly, and mistakes are going to be made as a result.”

LATEST INSIGHTS:

Our data and analytics team has developed a number of creative methodologies and frameworks that measure and benchmark the innovation that’s reshaping the payments and commerce ecosystem. **Check out the latest PYMNTS report on healthcare digital identity.**




DOWNLOAD NOW



PYMNTS.com

DIGITAL IDENTITY LIFESTYLE CAPSULE
2018 HEALTHCARE EDITION

RELATED ITEMS: B2B, B2B PAYMENTS, BANKS, COLLABORATION, CYBERATTACK, CYBERGRX, CYBERSECURITY, DATA BREACH, FINTECH, NEWS, RISK, RISK MANAGEMENT, RISK MITIGATION, SECURITY, THIRD-PARTY RISK

 SHARE  TWEET  SHARE  SHARE  PRINT  EMAIL
