



OMNI

SECURITY

AND AUTHENTICATION

SEPTEMBER 2018

REPORT

PYMNTS.com **ca**
technologies

How RBC Is Improving Its **Bank Security Intelligence**

Using AI to make
authentication strong
and simple

– Page 7 (Feature Story)

U.S. Department of Treasury
calls on congress to pass
cybersecurity laws

– Page 11 (News and Trends)

How banks build,
analyze and use
customers' digital profiles

– Page 15 (Deep Dive)

TABLE OF CONTENTS



REPORT

03

WHAT'S INSIDE

The latest omni security and authentication developments, including how demand for speed and convenience is putting pressure on FIs in the wake of high-profile security breaches

07

FEATURE STORY

How RBC Is Improving Its Bank Security Intelligence

Martin Wildberger, executive vice president of innovation and technology at Royal bank of Canada, on using emerging technologies to offer customers simplified, secure solutions

11

NEWS AND TRENDS

The latest headlines from around the space, including new debuts in the omni security and authentication industry

15

DEEP DIVE

How Banks Use Data To Build Customer Profiles

PYMNTS explores the ways FIs use customer data and AI to guard against fraud.

17

ABOUT

Information about PYMNTS.com and CA Technologies

ACKNOWLEDGMENT

The Omni Security and Authentication Report was done in collaboration with CA Technologies, and PYMNTS is grateful for the company's support and insight. [PYMNTS.com](https://pymnts.com) retains full editorial control over the findings presented, as well as the methodology and data analysis.

WHAT'S INSIDE

Modern consumers expect to seamlessly move across channels and go about their business without security concerns, whether checking bank account balances on smartwatch screens, transferring money to friends using smart speakers or shopping in the moment on social media platforms.

Enabling this seamless omnichannel experience can create security gaps and new opportunities for cybercriminals, however — particularly those who already have access to troves of consumer data, thanks to the growing number of security breaches and the amount of data available via the dark web.

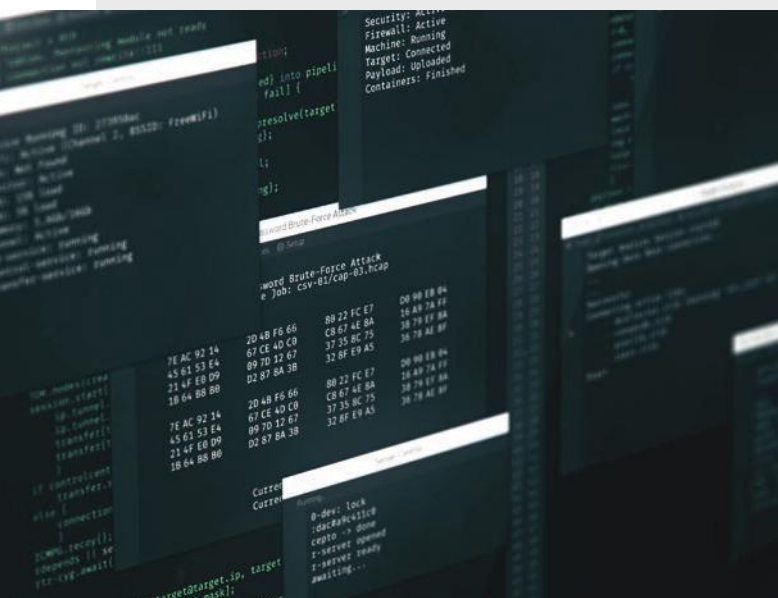
Credit reporting agency Equifax [suffered](#) a massive data breach just this past year, one which impacted nearly 150 million customers. It disclosed many consumers' full names, birth dates, addresses, Social Security numbers and even some 250,000 credit card account numbers.

Equifax was not alone, though. Fraudsters [attacked](#) Verizon Wireless, accessing the personal data of more than 14 million customers. Uber, too, suffered bad actors' wrath, disclosing in November 2017 that hackers had [stolen](#) nearly 60 million riders' and drivers' information. Even the government was within fraudsters' reach, as a Republican National Committee breach [exposed](#) roughly 200 million people's voting data.

All told, companies and consumers lost more than \$1.4 billion to more than 300,000 reported cyberattacks last year, forcing banks and merchants to [seek out](#) improved security and authentication capabilities to protect their customers, according to the Federal Bureau of Investigation's "2017 Internet Crime Report."

Enabling a seamless customer experience while also protecting data from bad actors is a battle financial institutions (FIs) and merchants must constantly fight, particularly in the wake of these and several other high-profile breaches. They're now turning to real-time authentication processes and profile data to verify consumers' identities without slowing down or complicating that experience.

Consumers crave convenience when doing business online, as evidenced by a recently conducted PYMNTS study. It found that 70.5 percent of those surveyed cited easy use as the most important feature of authentication





processes, 63.6 percent for convenience and 61.6 percent for speed. By comparison, just 44.6 percent considered stringent data security features to be the most important element, and 32.0 percent preferred high fraud protection levels.

What's more, PYMNTS found that overly complex authentication and checkout processes lead many consumers to rethink their online purchases entirely.

Other sources boast similar findings. Half of the consumers credit protection agency TransUnion [surveyed](#) for a recent report abandoned a digital cart after being confronted with a CAPTCHA sequence. The same study found that 28 percent of consumers gave up on online orders because the checkout processes were "too long/complicated," and a significant portion did so because the site required them to enter too much

personal information or to create an account to complete a transaction.

So, how can banks and merchants balance offering a convenient, seamless experience with stringent security and authentication?

ENTER THE OMNI SECURITY AND AUTHENTICATION REPORT, A CA TECHNOLOGIES COLLABORATION.

Designed to give readers an overview of the latest omni security developments, data, news and trends, this report will follow as tools are unveiled to protect consumers and provide them with a convenient online shopping experience. It will also present new data on consumer behaviors, habits and preferences, working to answer banks' and merchants' common authentication

questions: How well do you know your customers? What does it take to know your customers? Which authentication processes do your customers prefer?

Each edition of this report will focus on a different aspect of the space.

This inaugural issue examines how banks build, analyze and otherwise utilize customers' digital profiles; the ways they use data, risk analytics and neural networks to build a complete customer profile; and how that data enables various use cases, such as opening credit accounts, mortgage lending and wire transfers. It will also consider the ways customer information allows for other features' seamless operation — product histories or recommendations, for example.

Future editions will cover how banks leverage data to help customers utilize their products and features, and how payment standards like 3-D Secure authenticate users and work as a retail transaction onramp. They will also discuss how banks, merchants, processors and other stakeholders can leverage the data received from devices and cards to improve decisioning on any channel requiring a risk assessment — and do so before authenticating and approving a transaction — among other topics.

Each issue of the Omni Security and Authentication Report will contain an overview of major security and fraud prevention headlines in a News and Trends section (p. 11), offering readers a more comprehensive look into the notable trends shaping the market. It will also include a feature story (p. 7) packed with insights from important thought leaders, players and stakeholders, as well as a data-rich Deep Dive (p. 15) exploring relevant innovations in the space.

Enjoy the report!



\$38.719 MILLION

Projected value of the global neural network market by 2023

5 FIVE FAST FACTS

135%

Year-over-year increase in the volume of bank data available via the dark web

86%

Share of companies targeted by cyberattacks in the past 12 months

40%

Portion of bank sales made through digital channels in 2017

26%

Projected CAGR of the neural network software market through 2021

RBC TAKES

AN INTELLIGENCE-DRIVEN
TO BANK SECURITY



THE NUMBER OF CONSUMERS

visiting bank branches is [set](#) to decline by 36 percent over the next five years, while mobile banking usage is projected to increase by 121 percent.

The consumers turning away from bank branches and toward new connected channels are doing so in search of increased ease and convenience. The ability to bank on the go, across a range of connected channels, isn't just giving consumers and companies new ways to interact and do business, however. It's also presenting opportunities for fraudsters and cybercriminals, and bad actors are taking advantage.

According to recent [research](#), fraudsters stole more than \$7 billion from consumers and companies in 2016 alone, and did so on the backs of new technology and high-profile data breaches. Fraud rates are expected to skyrocket, too, with researchers [projecting](#) a nearly 200 percent increase within the next five years.

Cybercriminals are now making their gains through more sophisticated methods of attack. This means that those in charge of safeguarding consumers and merchants need a smarter approach when fighting fraud, one that incorporates emerging technologies and is driven by data about both customers' and fraudsters' habits.

In a recent interview with PYMNTS, Martin Wildberger, executive vice president of innovation and technology at [Royal Bank of Canada](#) (RBC), explained how the bank is using AI, machine learning (ML), neural networks and other innovations to fight fraud and protect customers.

"We're already using AI to analyze underlying patterns in complex market environments, and we're enhancing client security through biometrics and fraud detection algorithms," he said.

SMARTER SECURITY

Consumers want to access banking services online or on their phones, and they expect to do so without being put through a lengthy or complex authentication process. Fraudsters are becoming more sophisticated in how they

“We’re
enhancing
client security
through
biometrics
and fraud
detection
algorithms.”

target banks and consumers, though, meaning FIs have been forced to step up their efforts to stop them.

As a result, FIs are looking to learn more about their customers' habits and preferences, including how they typically manage their money – or, more importantly, how they don't. Banks can use this information to rapidly screen transactions, especially with AI and ML, and identify patterns that indicate bad actors are wreaking havoc on a person's financial life. This can all be done without the consumer having to lift a finger, enter a password or perform any other identity-verification measure.

For its part, RBC is using AI and ML to better understand its clients, find new insights and offer more personalized solutions and suggestions to clients. It is also looking to

further increase its use of neural networks, and actively investing in research and development. The bank opened its Toronto-based Borealis AI research lab in 2016 to accelerate the development of new use cases.

"RBC is aiming to push the boundaries of the science around machine learning," Wildberger added. "We are researching and developing ways to address cybersecurity, fraud management and biometric authentication using AI. In fact, we're continuing to innovate to enhance our capabilities and keep pace with the fast-changing threat landscape."

The company also provided support for the establishment of the [Vector Institute](#), which made its debut in 2017 and is staffed by Canadian AI, ML and neural networks experts.



“we’re continuing to innovate to enhance our capabilities and keep pace with the fast-changing threat landscape.”

BALANCING SECURITY WITH SIMPLIFIED EXPERIENCES

Consumers care how financial firms are working to protect their money and safeguard sensitive information. Eighty percent of those surveyed recently [told](#) researchers they believe protecting personal data should be a “top concern” for their FIs.

Consumers also crave convenience, however, even at the expense of security. Recent PYMNTS research found that 70.5 percent of those surveyed cited ease-of-use as the most important feature of an authentication process, while 63.6 percent cited convenience and 61.6 percent said speed. Just 44.6 percent considered stringent data security features to be the most important element, and 32.0 percent preferred high fraud protection levels.

As such, banks and other financial firms must work to offer stringent security – without sacrificing the convenience of customers’ experiences.

RBC forms profiles using data about customers’ habits and preferences to provide a safe and simple experience.

Transaction data is then automatically checked against these profiles without slowing customers down or asking them to complete complicated identity checks. Transactions that do not match pre-established patterns and habits will be rejected or flagged for further review.

The company plans to work with both internal developers and corporate partners to find other use cases for emerging technologies going forward, allowing it to offer a combination of simplicity and security. RBC has invested nearly \$4 million as part of AI and ML development partnerships with the Ben Gurion University’s Cyber-Security Research Center in Israel.

“This funding will support the development of adversarial AI, including ML-based cyber mitigation techniques,” Wildberger explained.

FIs will likely continue to innovate and create new opportunities through technology, but it appears cybercriminals are remaining eager to develop their own sophisticated methods to take advantage of those same opportunities.

NEWS & TRENDS



USING DATA TO BETTER KNOW CUSTOMERS

FACEBOOK ASKS BANKS FOR CUSTOMER DATA

As part of a recent effort to offer a wider array of personalized services to its users, Facebook has asked banks to share consumer information like checking account balances and card transactions. The company plans to use the data to develop features allowing users to receive fraud alerts and view account balances, according to [reports](#).

This news comes amid surging concerns surrounding the social networking site's use of data, particularly following allegations that market research firm Cambridge Analytica improperly collected users' personal data and utilized it to help elect U.S. President Donald Trump. Facebook CEO Mark Zuckerberg appeared before Congress to testify about the alleged misuse of data as a result.

NEW DATA HEADED TO BANKS, THANKS TO UPI 2.0

Indian banks are tapping into an upgraded version of the country's Unified Payments Interface (UPI) consumer-facing mobile app, and doing so to build stronger, more accurate customer profiles. The revised app includes overdraft credit line capabilities, which industry experts claim will help FIs access useful data on flow-based lending products. It is also [expected](#) to help consumers build their credit and give banks more data on their financial histories, according to an unnamed observer. What's more, access to the app's transaction and customer data will allow private banks — HDFC Bank, ICICI Bank and YES Bank, among others — to use it with internal algorithms and build customer profiles, even for those who have not yet done business with them.

OPEN BANKING DATA ATTRACTS GLOBAL ATTENTION, INVESTMENT

Other global financial ecosystem companies are also working to better secure and utilize customer data.

German open banking tech provider Deposit Solutions recently [received](#) \$100 million in funding, the second-largest round ever received by a German FinTech player. Its solutions work to connect “more than 70 banks from 16 countries” to more than 30 million consumers.

Another recent deal involved Equifax and a strategic alliance with digital consent management and open banking platform provider consents.online. The pair plans to develop data sharing solutions for the U.K.’s open banking initiative, enabling consumers and small and medium-sized businesses (SMBs) to provide organizations with consent to access financial data and build customer profiles.

As many as two-thirds of North American FIs view open banking and data sharing capabilities as “competitive imperatives,” according to recently released research. This likely foreshadows an increase in upcoming open banking and data sharing initiatives and offerings.

AN INTELLIGENT APPROACH TO SECURITY

BANKS BET ON AI FOR RISK MANAGEMENT

While data collection is key for FIs offering improved services, it doesn’t do much good if not leveraged properly. Several banking players are now [looking](#) to pair customer data with AI, thereby improving risk management capabilities, and 15 Indian banks recently rolled out AI-powered risk management software from Bengaluru-based provider GIEOM.



Bank of Maharashtra, Central Bank of India, Federal Bank, IDFC Bank, IndusInd Bank, South Indian Bank, the State Bank of India and YES Bank, among others, will all use the software, as well as know your customer (KYC) and anti-money laundering (AML) processes to better leverage customer data and make decisions regarding fraud or other unusual circumstances. The solution will also offer bank executives regulatory issue alerts.

“No one can check every loan that has been given and also ensure that the multiple human business controls are followed,” noted John Santosh, GIEOM founder, but AI solutions can help lift some of the burden.

AI TO BOOST FRAUD PREVENTION

The U.S. government is also exploring personal data and AI usage regulation. In a recent [report](#), the Department of Treasury called on Congress to organize federal summits and interagency efforts centered around AI, and for lawmakers to work with FinTech

firms on regulations for “data sharing, standardization, security and liability issues.” It advocated for Congress to enact a federal data security and breach notification law, as just 13 states currently have such regulations – each with differing requirements. These apply to companies that do business in a state, with or without offices there, and a federal move would “employ uniform national standards that preempt state laws,” among other attributes.

BIOMETRIC BUSINESS

SOCIETE GENERALE UNVEILS ONLINE BIOMETRICS

While the U.S. Treasury sets its sights on AI, French multinational bank Societe Generale is hoping to leverage another emerging technology for data security and protection: biometrics. It [announced](#) late last month that it would add facial recognition to its authentication offering after coming to an agreement with the French Commission nationale de l’informatique et des libertés on data privacy laws. The bank will now use biometric data to enable consumers to log in with a “selfie.”

In a blog post, Societe Generale said the data would be “encrypted and illegible” during the verification process, protecting it from being snatched up by bad actors. It also noted that 10 percent of its new accounts are being authenticated using biometrics, a number the company expects to see grow to 30 percent in the next two years.

BEHAVIORAL BIOMETRICS ON THE RISE

While Societe Generale works with physical biometrics, others are turning to behavioral. The Royal Bank of Scotland (RBS) is among the FIs and merchants [monitoring](#) website and app visitors with the help of behavioral biometrics, having implemented the technology for its wealth management clients two years ago. The solution records customer interactions with keyboards, touchscreens and other access points, creating data that can later be used to construct a consumer habits and preferences profile. This information can then be leveraged for authentication or recommendations when consumers revisit a site.

The RBS capability was created in collaboration with Israel-based financial security firm BioCatch, which secured \$30 million in an investment round led by Maverick Ventures earlier this year. That round also included participation from American Express Ventures and NexStar Partners, among other firms.



BLOCKCHAIN BULLETINS

CAPITAL ONE EYES BLOCKCHAIN AUTHENTICATION

Banks are also investing in blockchain solutions. Capital One [filed](#) a patent application with the U.S. Patent and Trademark Office last June, hoping to use the technology to secure user authentication methods for banking security. It aims to create a blockchain-based system that receives, stores and retrieves encrypted user authentication data, according to a Coinbase report. The filing was released in mid-August.

Capital One's patent application describes a "distributed, non-reputable record of authentication interactions" that allows users to verify themselves across various platforms by sharing limited personal information. The system would authenticate or reject the user based on blockchain-secured data, which the bank claims would reduce FIs' time and resource burdens when onboarding clients. It aims to appeal to customers who resent having to authenticate themselves as they interact with multiple financial firms. These firms "may, therefore, benefit from a collaborative authentication system that handles authentication interactions for multiple institutions," according to Capital One.

NEURAL NETWORK NEWS

NEURAL NETWORK MARKET TO HIT \$38.7 MILLION BY 2023

The global market for neural networks, a form of AI involving a series of algorithms, will [reach](#) \$38.719 million within five years, according to recent projections, and see growth in interest among both FIs and players

from a range of industries. This would represent a compound annual growth rate (CAGR) of roughly 28 percent through 2023, one fueled by increased investment from banking, financial services and insurance players.

The neural networks industry is also driven by demand for cloud-based solutions, as well as a growing focus on spatial data and analytical tools. An increase in the number of applications is expected to boost the market's value, though a lack of professionals trained to work with and use the technology could prevent further expansion.

BANKS INCREASE INVESTMENTS IN NEURAL NETWORKS

Sparkassen, Germany's state-run savings bank, recently [announced](#) plans to invest in neural networks to remove manual paperwork. The FI is now using the networks to automate the completion and review of handwritten forms, leading to improved bank-reported efficiencies. Its neural network has a 98 percent success rate and is trained in handwriting analysis and recognition, according to IT service provider Andreas Totok. What's more, it is continuing to learn and improve its recognition rate.

SOPHOS INTRODUCES INTERCEPT X TO BLOCK CYBER ATTACKS

FinTechs are also turning to neural networks to boost their offerings and protect their servers. IT security solutions provider Sophos Lab has [announced](#) it would begin using them to identify and halt potential malware attacks on banks and other FIs. Its Intercept X neural network is designed to detect new and previously unseen malware or unwanted applications, according to a press release. It can constantly update its abilities, too, identifying critical attributes of suspicious transactions, blocking commonly used fraud techniques and preventing attackers from leveraging known vulnerabilities, among other use cases.

DEEP DIVE:

HOW BANKS USE DATA TO BUILD CUSTOMER PROFILES

Connected devices' popularization and widespread adoption have given businesses in all industries access to an abundance of behavioral insights. After all, more than 4 million connected devices produce more than 2.5 exabytes — equivalent to 2.5 billion gigabytes — of data per day, according to recently published [research](#). That's a greater amount of data generated over the past two years than ever before.

Banks and FIs can now tap into this data to learn about the services customers value most and how they can keep consumers happy. It gives them a deeper look into who their customers are, too, including where, when and how they typically interact with bank interfaces. The data further allows FIs to build personalized profiles based on customer habits, then use said profiles to authenticate and validate identities and transactions — which will only be more helpful to customers. Personalization has become an expected element of the experience.

USING DATA TO BUILD A PROFILE

Customer profiling has become an essential asset of FI's security and authentication suites. Banks begin building profiles using internal data, like customer-generated revenue, products and channels used most often and how quickly he or she responds to notifications. They then supplement this information with third-party data, which helps them understand how a customer interacts with other companies or organizations.

Financial firms can create a rich, full picture of a customer's habits, both online and offline, in that profile. Profiles can then be analyzed and used to make tailored decisions, including which promotions to offer, which products to push most heavily and how legitimate his or her transactions look.

These processes are typically automated, helping FIs more quickly identify suspicious transactions and often catching fraudsters in the act. Automation also

allows consumers to enjoy a seamless experience while benefiting from strong security and authentication. In addition, consumers get to avoid frictions like security questions or long, complicated authentication checks because data is automatically collected and analyzed.

ANALYZING AND AUTHENTICATING

Customer profiles can also be used to protect money. Each time a customer logs into an online or mobile bank account, or attempts to complete a transaction, that action is compared to his or her profile. If the transaction falls outside typical habits, it is flagged for further authentication and evaluation.

More than 2.5 exabytes per day might sound like a colossal amount of data, but banks will likely have more of it coming their way before too long. Consumers are increasingly using connected devices to view their bank account balances, send money to friends and family via person-to-person (P2P) apps like Zelle or Venmo

and even apply for loans or other bank products — all of which becomes usable data. This additional data should allow FIs to build deeper consumer profiles and better understand their habits and preferences.

Stringent security and protection will be crucial for companies in the financial services space as FIs and their customers continue to conduct more business via online, mobile and other digital channels. Seventy-five percent of companies were victims of fraud in the past year, according to McKinsey and Company [data](#), and 73 percent of financial professionals reported being targeted — a noticeable increase over previous levels.

It appears investing in developing and analyzing customer data and digital profiles may hold the most promise, particularly for firms looking to protect themselves against cybercriminals and improve efficiency in the banking space.

75%
of companies
were **victims
of fraud**
in 2017.



about

PYMNTS.com

[PYMNTS.com](https://pymnts.com) is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.



CA Technologies creates software that fuels transformation for companies and enables them to seize application economy opportunities. Software is at the heart of every business in every industry. From planning and 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 www.ca.com.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at omnisecurity@pymnts.com.

disclaimer

The Omni Security and Authentication Report may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.

You agree to indemnify and hold harmless, PYMNTS.COM, its parents, affiliated and related companies, contractors and sponsors, and each of its respective directors, officers, members, employees, agents, content component providers, licensors, and advisers, from and against any and all claims, actions, demands, liabilities, costs, and expenses, including, without limitation, reasonable attorneys' fees, resulting from your breach of any provision of this Agreement, your access to or use of the content provided to you, the PYMNTS.COM services, or any third party's rights, including, but not limited to, copyright, patent, other proprietary rights, and defamation law. You agree to cooperate fully with PYMNTS.COM in developing and asserting any available defenses in connection with a claim subject to indemnification by you under this Agreement.