SMARTER PAYMENTS TRACKER™

JUNE 2018: SECURITY

FIS

PYMNTS.com

TABLE OF CONTENTS

ACKNOWLEDGMENT

The Smarter Payments Tracker™ is powered by FIS, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the findings presented, as well as the methodology and data analysis.

WHAT'S INSIDE

BANKS, FINTECHS AND RETAILERS

are working closely together to innovate and improve the pace, efficiency and intelligence of payments.

These collaborations are helping banks move at a faster pace, but financial institutions (FIs) are facing growing pressure to ensure that faster payments are properly authorized by the intended parties and used for legitimate purposes. They're also seeing new threats emerge from a host of bad actors as payments become smarter.

In retail payments, for instance, some of the most serious security concerns include risks of fraud, a breakdown in operational procedures and legal liability. This edition of the Smarter Payments Tracker™ focuses on new security challenges that are emerging as more companies and banks work together.

Around the smarter payments landscape

A heightened risk of data breaches has consumers in North America on edge. A recent survey from cybersecurity firm Kaspersky Lab found 81 percent of Americans and 72 percent of Canadians are stressed about a recent pattern of data breaches. Based on input from 2,000 North

American consumers, it pointed to consumers' overall lack of awareness on how to protect themselves from a data breach.

Speaking of a lack of awareness, a study from credit monitoring service Credit Karma has found that 65 percent of its users have experienced a data breach whether they realize it or not. The company recently partnered with cybersecurity firm SpyCloud to scan the Dark Web and roughly 4.5 billion breaches for its customers' personal data.

Meanwhile, a new type of distributed denial of service (DDoS) cyberattack is relying on a well-known vulnerability. Cybersecurity firm Imperva revealed the DDoS attack in a proof of concept (PoC) highlighting how cyber criminals can exploit Universal Plug and Play (UPnP) networking protocol weaknesses to go undetected, thereby making it difficult for IT professionals and companies to pinpoint the source of the attack. The finding could have broad implications for the Internet of Things (IoT) ecosystem.

Why making payments smarter also means making them safer

Account takeovers are fraudsters' new favorite cybersecurity breach. Usage has tripled over the past year, and losses have topped $5 billion. Cybercriminals are drawn to the technique because it is often easier to pull off than other cyberattacks — and more difficult for security forces to detect and stop.

What's Inside

In this month's Smarter Payments Tracker™ feature story (p. 10), PYMNTS caught up with Dave Endler, co-founder and president of security and fraud prevention solutions provider SpyCloud, to learn more about the rise of account takeovers and what can be done to stop them.

Deep Dive: DDoS attacks

Earlier this year, web hosting service GitHub experienced one of the worst DDoS attacks on record — but the company is not alone. Major FIs like Bank of America, Wells Fargo and PayPal have been targeted by similar attacks over the years, costing them hefty amounts for their disrupted service. This month's Deep Dive (p. 19) examines the growing threat of DDoS, the toll they can take on companies and the steps firms can take to mitigate potential threats.

81% OF AMERICANS & **72%** OF CANADIANS

are stressed about a recent pattern of data breaches.

EXECUTIVE INSIGHT

Faster payments can make it harder for FIs to detect bad actors among the good ones. How can they stay on top of more quickly preventing fraud?

"Faster payments don't necessarily mean more fraud, but planning how you'll provide administrative support and 24/7/365 monitoring to adapt to the new demands of speed becomes even more crucial.

Whether you opt to manage your fraud prevention efforts with your own resources or through a partnership with a skilled provider, preventing fraud in a real-time environment demands that all of the systems you rely on to process payments are real-time enabled, from end to end. For some financial institutions, this may require an adjustment to existing operations — including real-time notifications and settlement, and comprehensive back-end support — to perform in a real-time environment.

It also important to understand that once latency in transaction processing and settlement go away, authentication risk remains a danger. A robust digital identity solution that works in real time, and layers frictionless verification capabilities like biometrics, device ID and geospatial data, is the most effective way to resolve authentication risk."

ERIC KRAUS,
vice president and general manager of fraud management at FIS Payments

5 FIVE FAST FACTS

65%

Share of Credit Karma users who have experienced a data breach, whether aware of it or not

80%

Portion of data breaches that initially occur with SMBs

$7.5 BILLION

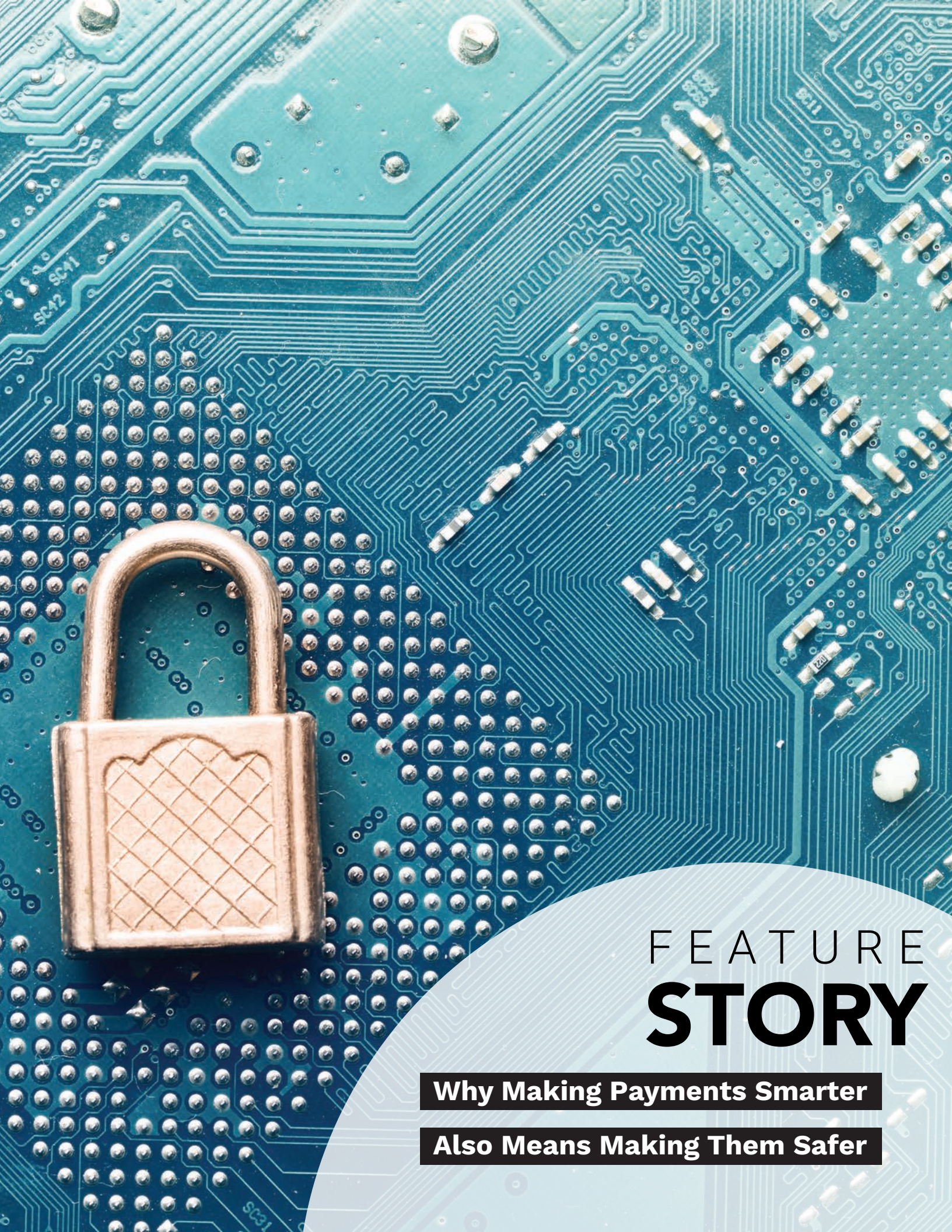
Projected value of the cyber insurance industry by 2020

1,570

Number of U.S. data breaches reported in 2017, up 44 percent from 2016

30%

Year-over-year increase in cyberattacks across Europe in Q1 2018



FEATURE

STORY

Why Making Payments Smarter Also Means Making Them Safer

WHY

Making **Payments Smarter** Also Means Making Them SAFER

Cybercriminals have a new favorite weapon in their quest to allude regulators, law enforcement and corporate security departments: account takeovers.

Recent research reveals account takeovers have risen by 300 percent over the past year, with losses topping $5 billion. What's more, these attacks can often have far-reaching and long-term implications for those affected. Victims paid an average of $290 out of pocket in 2017, and spent approximately 15 hours resolving takeover-related fraud.

There's good reason why cybercriminals are turning to the technique, according to Dave Endler, co-founder and president of security and fraud prevention solutions provider SpyCloud. In a recent interview with PYMNTS, he noted that account takeovers are often easier to pull off compared to other cyberattacks, causing more fraudsters to use the technique. These attacks are also more difficult for security forces to detect and stop.

"It's much more straightforward for a criminal to compromise someone's payment account that could be linked to a credit card than for them to try to steal or gain access to use that credit card," Endler said, adding that the tools that make these attacks possible are "accessible to people who don't necessarily have a lot of technical acumen."

The rise of account takeovers

One of the main reasons cybercriminals have embraced account takeovers is the wide array of

> The level of sophistication required to compromise someone's online account is **very low**, especially in the wake of all these mega-breaches coming out.

information the attacks provide, usually including all the data and credentials they would need to misrepresent a consumer.

Making matters easier for fraudsters — and more complex for those fighting to stop them — is the fact that cybercriminals can purchase account credentials via the black market, Endler explained. That means anyone can use account takeovers to commit fraud. After all, companies often verify their users through data like home addresses, IP addresses or answers to security questions.

Recent breaches at big name companies have only made the problem worse, he added. Even if a payment service hasn't experienced a breach that exposed users' personal information, those at social networking or online shopping platforms can reveal usernames, email addresses and

passwords consumers use with more than one platform.

"The level of sophistication required to compromise someone's online account is very low, especially in the wake of all these mega-breaches coming out," Endler said. "It creates and exacerbates this collateral damage. Even if PayPal has not experienced these types of breaches, a breach, say, to LinkedIn, could cause the security of PayPal's users to be compromised if they're using those same passwords. That's account takeover 101."

Of course, that same black market also drives the value of these stolen accounts.

"Many times, criminals will, at scale, be able to compromise a multitude of accounts in different verticals," he added. "Not just payments, but banking accounts and technology accounts that might have some sort of virtual points associated with them. So, [that includes] the hospitality industry or anything like Starbucks or Netflix or Hulu — anything where an account offers some sort of value to someone, whether financial value to criminals or resell value of the account on some other market."

Keeping consumer accounts secure

A cyberattack that exploits a low barrier of entry could seem like an unstoppable enemy, but Endler said there are steps consumers and companies can take to better protect themselves against account takeovers.

UNDER THE HOOD

Companies are continuously exploring new ways of fighting fraudsters and securing payment details. Offering a robust system of security and authentication protocols does no good if consumers can't — or choose not to — use the features offered to them, however. In a recent interview with PYMNTS, Dave Endler, co-founder and president of security and fraud prevention solutions provider SpyCloud, discussed how consumers impact the effectiveness of online security features.

"When you talk not just about security of payments, but [also about] general information security, the weakest link is the human factor.

You can invest a lot in technology, but, at the end of the day — even if you enforce password management, even if you enforce a lot of good hygiene when it comes to people creating and using their accounts — if they use a personal email to sign up for a Dropbox account and use the same password they used on five other sites, and one of those sites gets hacked? That Dropbox account can lead to corporate exposure even though the corporation has no visibility into Dropbox, because [the company is] not necessarily managing it, and the person's personal email address was the one that was used.

It is becoming a little bit more sophisticated… but the human link is always the weakest… when it comes to passwords, and that has continued to be one of the biggest, if not *the* biggest, way that criminals are breaking into organizations today. That's backed up by a couple of recent reports. The Verizon data research report from 2018 classified the use of stolen credentials as the top action that happens in a breach, for example."

Companies can decrease or eliminate passwords for user authentication, for example, because passwords are one of the biggest ways criminals are breaking into organizations today. Consumers can take steps to better guard themselves, too, like following the one-account-per-password rule to protect their accounts.

"If everyone used a separate password on every single site, and used password managers and two-factor authentication, that would set a very high bar," Endler said. "But, the reality is not [many] people are doing that. I'd gather it's in the 10 percent range, if that."

The same is true of security questions and answers, which consumers often reuse time and time again. SpyCloud recently partnered with Credit Karma to offer a solution that can eliminate security questions with answers that have been exposed in a security breach.

Endler recommends that banks, FinTechs and other platform providers work to determine which users' accounts have been exposed elsewhere on the web. This can help companies proactively reset their account details and prompt them to step up their security settings going forward.

It's important for companies to act quickly once a breach of either their own systems or of those used by their customers is discovered, he

added. After all, account details remain vulnerable forever once they're exposed.

"Being able to take proactive action against these accounts and prevent a criminal from even getting access in the first place is key," Endler said. "The LinkedIn breach form 2012? Those passwords are freely available for download and have all been unencrypted — and [they] are still relevant to this day. People's cat's names, their significant others' [names], their children's names — [those] don't change very often. All those continue, to this day, to lead to compromises of online accounts."

Those long-term impacts mean stopping account takeover is a tall order, but it's a task that's crucial to tackle, he added. After all, the allure will only become more lucrative to fraudsters as consumers spend more time and money online.

NEWS AND TRENDS

SCANNING FOR SECURITY

Credit Karma to scan Dark Web for customers' data

Many consumers might be unaware if their data has been compromised or accessed on the Dark Web. Credit score and identity monitoring service Credit Karma is hoping to help make them more aware, recently partnering with cybersecurity firm SpyCloud to scan approximately 4.5 billion breaches for its users' personal data. The scans will also include data available on the Dark Web, aiming to reduce consumers' anxieties about data theft. Credit Karma recently reported that 65 percent of its estimated 80 million-plus users in the U.S. and Canada have experienced a data breach — some of which do not know that the incident even occurred.

Keeping pace with fraud in real-time payments

As payments get faster, companies are realizing they need equally fast alerts if data breaches occur in order to prevent fraud. Gary Kearns, Mastercard's executive vice president, and payment company Vocalink's director of financial crime solutions, David Divitt, recently spoke with PYMNTS' about the opportunities faster payments present for fraudsters and criminals. Kearns noted faster payments do not necessarily mean more fraud. Fraudsters can now take advantage of real-time digital payments to launder funds in minutes or hours instead of days, though, and banks have a hard

65%

Portion of the roughly 80 million Credit Karma users in the U.S. and Canada that have experienced a data breach **— SOME OF WHICH DO NOT EVEN KNOW THAT THE INCIDENT OCCURRED**

time seeing outside their own four walls to detect bad actors against normal-looking account activities. FIs need to take a "network-level view" of transactional activity, Divitt added, using machine learning and artificial intelligence (AI) to spot the signs that other prevention solutions might miss.

NEW RISKS & SOLUTIONS

How a new DDoS attack avoids detection

A new type of DDoS attack is counting on a known weakness in UPnP networking protocols to be overlooked by administrators, thereby evading common detection rules. The DDoS was revealed as a PoC, compiled by researchers at cybersecurity firm Imperva, which highlighted how cyber criminals can manipulate port mapping to hide the source. This makes it more difficult for affected companies to address it.

UPnP protocols are still used for device discovery purposes, and are commonly tapped by IoT-enabled devices. Vulnerabilities in the protocols are well-documented and include poor default settings, lack of authentication and UPnP-specific remote code execution, all of which make connected devices vulnerable. Despite these issues, the protocols are still widely employed due to their ease of use.

Massachusetts needs cybersecurity professionals

The commonwealth of Massachusetts' cybersecurity community is facing a different type of problem: a lack of qualified professionals. Bay Path University president Carol Leary, Ph.D., recently told MassLive.com that the lack of cybersecurity experts is causing a "severe talent gap" in the area.

Leary made the comments while testifying before the Legislature's House Committee on Technology and Intergovernmental Affairs and the Joint Committee on Public Safety and Homeland Security. Small and medium-sized businesses (SMBs) are among the most vulnerable to cyberattacks, according to the reports, and many cannot keep up with the challenges of securing their networks. Delcie Bean, founder and CEO of technology consulting firm Paragus IT, noted two SMBs were forced to shutter after audits found they could not keep up with such IT demands. The Economic Development Council of Western Mass added that approximately 80 percent of data breaches first occur through SMBs, notably manufacturers.

B2B payments on path to security, speed

Businesses' cybersecurity is of growing concern, especially for those that engage with them. A

recent "Payments Pulse Data" report from payments company WEX found 75 percent of accounts payable (AP) professionals listed payment security as suppliers' top priority. Meanwhile, a separate report from TD Bank and consulting firm Strategic Treasurer noted companies are planning to step up their cybersecurity efforts, with 74 percent listing digital fraud as an increasingly important concern in 2018 and beyond.

Both reports indicate that cybersecurity is top of mind for most businesses, and also offer insights into their views on faster payments. WEX found 68 percent of AP professionals say speed

is important to their suppliers, while TD Bank and Strategic Treasurer saw more than 33 percent of businesses claim speed is as important as payment data accessibility. Both findings indicate that companies are working to walk the balance between cybersecurity and speed.

74%

Percentage of companies surveyed by TD Bank and Strategic Treasurer that say **THEY PLAN TO STEP UP CYBERSECURITY EFFORTS**

On that front, SMB bookkeeping solutions provider PeaCounts is launching a solution that relies on tokenization and blockchain to ensure B2B payment speed and security. Blockchain technology offers enhanced security for data that is stored and accessed by the solution, and cryptographic tokens will be used to facilitate decentralized payment verification, thus limiting access to sensitive account information and payment data.

CUJO raises more capital

Vulnerabilities in connected devices can allow cybercriminals or hackers to detect consumer information, meaning more opportunities arise as consumers become more connected. The average U.S. household has approximately 22 connected devices, according to

data from AI-powered software solutions provider CUJO AI. Its solutions aim to keep such devices safe by enabling network operators to secure home users and improve connected home experiences. CUJO recently gained some additional capital through a Series B funding round led by Charger Communications, an investment it will use to expand into global markets like North America, Europe and the Asia Pacific.

CYBERSECURITY BY THE NUMBERS

Cyberattacks up 30 percent in Europe

Recent data from risk solutions company ThreatMetrix indicates cybersecurity is a fast-growing need in Europe. Cyberattacks grew at a rate of 30 percent year over year in Q1 2018 alone, with

identity spoofing, stolen passwords and data being sold on the Dark Web becoming a huge problem. ThreatMetrix also noted that identity spoofing incidents more than doubled in Germany between Q1 2017 and Q1 2018, according to analysis of 1.9 billion transactions on its Digital Identity Network in Europe.

Americans, Canadians stressed by data breaches

Rising data breach activity is leading to rising stress levels among U.S. and Canadian consumers, according to a new survey released by cybersecurity firm Kaspersky Lab. Based on input from 2,000 North American consumers, the "State of Cyber-Stress" report found 81 percent of Americans and 72 percent of Canadians are anxious about a recent series of data breaches — and that a lack of awareness on how to effectively protect themselves was among the factors driving those levels.

"Many people still have no idea how to begin securing their devices from these threats, or what to do if they become a victim," said Brian Anderson, Kaspersky's vice president of consumer sales.

As a result, consumers are becoming increasingly anxious about cybersecurity. The survey found respondents are increasingly stressed about creating secure passwords and keeping track of the login information needed to access online accounts. Anderson urged technology companies to educate consumers on how to manage their data security, thereby helping to ease their anxieties.

For cyber insurance, attacks can be riskier than hurricanes

Companies that provide cyber insurance have their own reasons to be anxious, as cyber threats, like last year's WannaCry attack, are leading to rapid market growth. Cyber insurance is a

30%

Increase in European

CYBERATTACKS

as of Q1 2018

difficult industry to get right, though, according to Rotem Iram, CEO of cyber insurance and risk management solutions provider At-Bay.

The market for cyber insurance carries big risk, Iram explained in a recent interview with PYMNTS. In fact, Berkshire Hathaway CEO Warren Buffet noted providers could face at least $400 billion in insured losses due to a catastrophic cyberattack. It's especially challenging to predict the potential severity of future risks based on older technology, Iram said, adding that cyber risk is "at odds" with the traditional insurance industry business model for several reasons. Cyberattack-related risks are constantly changing, too, and vendors are frequently adding fixes to bugs. This makes it challenging for insurance companies to pinpoint exact risk assessments.

SECURING PAYMENT CARDS

NBK, Mastercard partner for biometric cards

The National Bank of Kuwait (NBK) is turning to biometrics to boost digital security, recently collaborating with payments processor Mastercard to pilot a payment card with embedded fingerprint sensors. The card is the first of its kind offered in the Middle East, according to a Mastercard news release, and is designed to improve consumers' online and in-store shopping experiences.

A cardholder must insert the card into a merchant's EMV-compliant point-of-sale terminal to use it, then place a finger on the embedded sensor. The scanner verifies the fingerprint against the template stored on the card. The cards also offer Selfie Pay with Mastercard, which enables users to authenticate payments by taking a selfie.

Mastercard gets behind SRC framework

In addition to delivering more secure payment card options to

Kuwait, Mastercard is also working to offer a consistent online and in-person payment experience. Jess Turner, North American executive vice president of the company's

digital payments and labs, said Mastercard is supporting payment solutions provider EMVCo's Secure Remote Commerce (SRC) framework.

SRC will scale digital payments acceptance and replicate the consistent experience shoppers have come to expect online, Turner explained. Paired with a single buy button, it will help mitigate friction associated with expired or stolen cards by creating an encrypted token that outlives the card number. The solution is not influenced by

these developments, she added. In fact, it will enable a more secure framework for digital transactions, as roughly 75 percent of cards in the U.S. can be tokenized.

75%

Portion of U.S. payment cards that

CAN BE TOKENIZED

DEEP DIVE

The Growing Threat Of DDoS Attacks

THE GROWING THREAT
Of DDoS Attacks

Interconnectivity among FIs aims to promote greater collaboration and competition in the financial services marketplace, with the ultimate goal of providing better services, products and options to consumers. As these FIs work closely together, though, they might also find themselves vulnerable to cyberthreats.

A DDoS attack is among the most serious of these threats. Multiple compromised computer systems launch attacks on one or several parts of an organization's infrastructure during a DDoS event, and that can include a server, website or other type of resource.

One of the worst attacks on record — by some accounts — occurred earlier this year. Web hosting solutions provider GitHub recently reported it had experienced an attack at a rate of 1.35 terabytes per second (Tbps), beating the previous record of 1.1Tbps.

Web hosting services like GitHub are not the only ones to experience DDoS attacks, however. Financial services companies around the globe have also been targeted in the past decade, including Bank of America, Wells Fargo, Capital One, HSBC and non-bank financial companies like PayPal. These attacks are estimated to have cost affected FIs $100,000 per hour of disruption.

The DDoS threat is likely to increase as cybercriminals become more sophisticated. The following Deep Dive examines how they work, the toll they can take on FIs and the steps banks can implement to guard against future DDoS threats.

The growing danger of DDoS attacks

A computer or connected device becomes compromised by malware during a DDoS event. The malware turns the infected devices into bots that can be used to perpetuate the malicious cyber event.

DDoS **ATTACKS** cost FIs an average of **$100,000** per hour of disruption.

There are several avenues through which a DDoS attack can wreak havoc on an organization. It could result in an HTTP flood, for example, which sees a large number of HTTP requests overwhelm a server. Protocol attacks, on the other hand, interrupt service by diverting resources away from firewalls, load balancers and other solutions that organize traffic across servers.

Recent research indicates DDoS threats are on track to become even greater and more sophisticated in coming years. They can exceed 1,000 gigabytes per second (Gbps), too, as the bots involved have grown more effective.

A 2016 attack by the Mirai botnet on online infrastructure services provider Dyn DNS — currently known as Oracle DYN — resulted in a massive flood of domain name server (DNS) queries across tens of millions of internet protocol (IP) addresses. The attack reached 400,000 bots and disrupted services to major companies, including Amazon, Netflix, Reddit, Spotify, Tumblr and Twitter.

There was good news when GitHub was hit earlier this year, though: It thwarted the attack in roughly 20 minutes. The event offered insights into the potential dangers to come, however. Unlike the Dyn attack, which reached its peak at 1.2Tbps of data, the GitHub attack reached 1.35Tbps. A few days later, another struck an unnamed U.S. service provider at a rate of 1.7Tbps.

Preparing for the worst

With the threat of DDoS attacks increasing — especially as attackers become more sophisticated and banks become more dependent on third-party providers (TPPs), interconnected platforms and web-based systems — banks, companies and governments alike now consider cybersecurity a top concern. Several players around the globe are now helping companies to prepare for DDoS and other types of cyber threats.

For example, Global Data Protection Regulations (GDPR) went live in Europe in May, requiring firms to implement a data handling strategy that meets a regulated level of oversight in terms of how they handle private data. Companies that operate in Europe are also required to have notification protocols in place in case of a data breach, and each region has been assigned data protection

authorities (DPAs) to conduct investigations or impose fines to enforce the measure.

As more banks and FIs collaborate on improved services for consumers, they are also encouraged to carefully monitor the partners with which they engage. Recent research finds consumers expect their banks and retailers to take stronger precautions, with a 2017 survey from Consumer Payment Card Data Security Perceptions noting 82 percent of respondents feel "banks, retailers and other organizations involved in the credit/debit card industry need to do more to protect their personal card data."

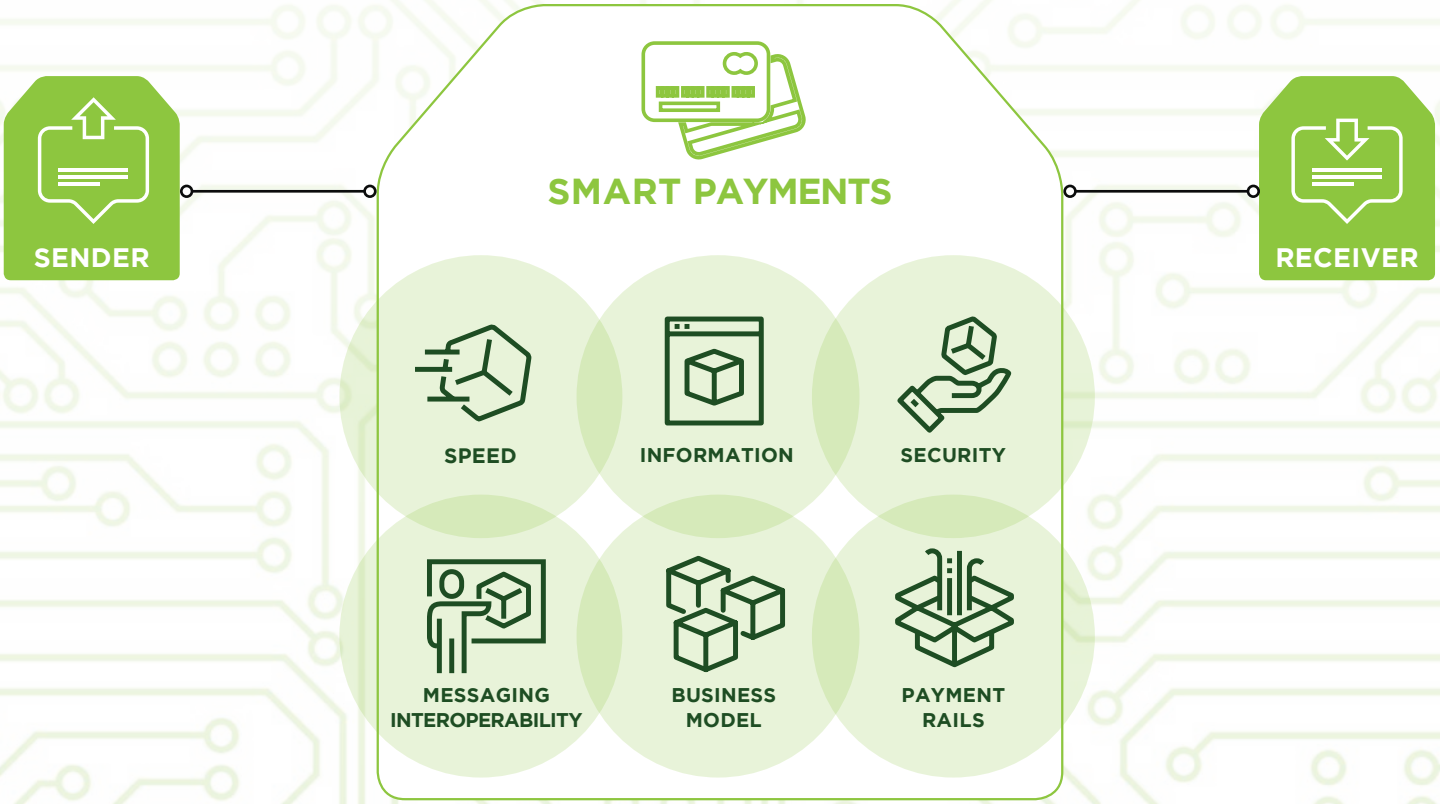
The takeaway from this survey is clear: Consumers want FIs and retailers to do more to protect their data as cyber pressures mount. This means organizations must invest in securing their networks, software, hardware and any other resource involved in the transmission and exchange of personal data or financial information.

A growing rate of collaboration is helping to make payments smarter, but FIs and retailers must still take the appropriate precautions to keep payments safe — especially given the havoc a DDoS attack can wreak.

SMARTER PAYMENTS ARCHITECTURE

The Smarter Payments Tracker highlights the latest trends at the intersection of smarter payments and authentication. Each monthly report explores one of the six tenets of the Smarter Payments Architecture, including messaging interoperability, speed, information, security, payment rails and the modality of B2B and B2C payments and their value.

THE ANATOMY OF SMARTER PAYMENTS ARCHITECTURE



about

PYMNTS.com

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 companies in payments share relevant information about the initiatives that make news and shape the future of this dynamic sector. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovations at the cutting edge of this new world.

FIS

FIS is a global leader in financial services technology with a focus on retail and institutional banking, payments, asset and wealth management, risk and compliance, consulting and outsourcing solutions. Through the depth and breadth of its solutions portfolio, global capabilities and domain expertise, FIS serves more than 20,000 clients in more than 130 countries. Headquartered in Jacksonville, Florida, FIS employs more than 55,000 people worldwide and holds leadership positions in payment processing, financial software and banking solutions. Providing software, services and outsourcing of the technology that empowers the financial world, FIS is a Fortune 500 company and is a member of Standard & Poor's 500® Index. For more information download the FIS Success Guide: Determining your entry point into the faster payments ecosystem.

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

disclaimer

The Smarter Payments Tracker™ 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.