FEATURE STORY

How Middle Eastern Merchants Can Keep Up With **Pandemic-Driven Privacy, Payment Shifts** – *Page 8*

NEWS & TRENDS

Saudi Arabia's FinTech ecosystem triples in size as its monetary authority approves permits for proofs of concept, testing – *Page 13*

DEEP DIVE

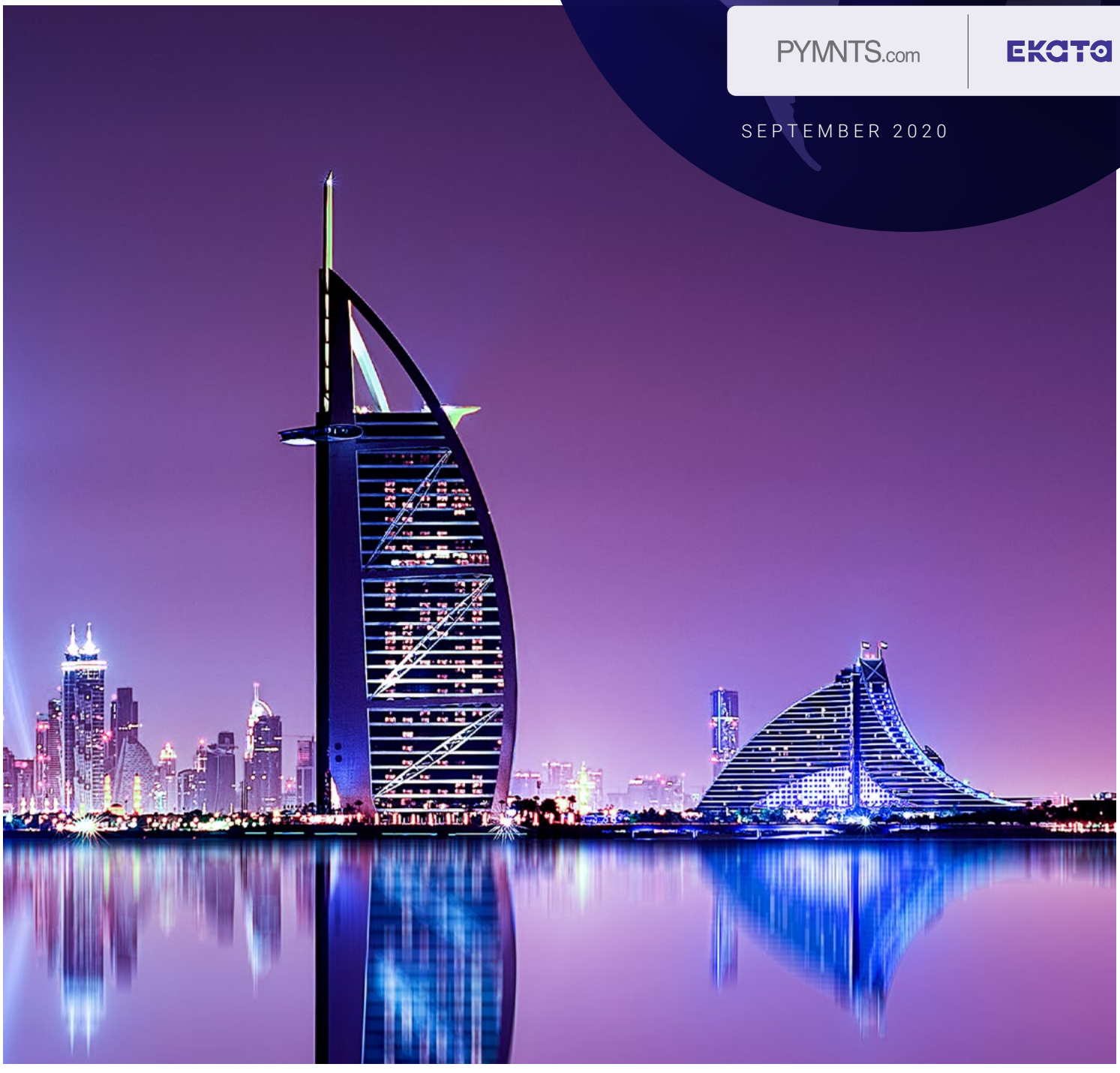
Why MENA regulators may need to upgrade their data privacy laws as the pandemic shifts users' online expectations – *Page 19*

Merchants Guide To Navigating

GLOBAL PAYMENTS REGULATIONS

PYMNTS.com | EKATA

SEPTEMBER 2020



Merchants Guide To Navigating

GLOBAL PAYMENTS REGULATIONS

PYMNTS.com | EKATA

TABLE OF CONTENTS

ACKNOWLEDGMENT

The Merchants Guide To Navigating Global Payments Regulations was done in collaboration with Ekata, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

WHAT'S INSIDE

The COVID-19 pandemic is not stopping open banking's development, but it does appear to be altering its course. More consumers, merchants and financial institutions (FIs) are scrutinizing open banking initiatives and the involved security and privacy measures as the health crisis pushes a growing share of commerce online. The long-term impacts of this migration could ultimately encourage lawmakers to examine their nations' regulatory standards and determine whether updates are needed to keep up with the digital shift.

Regulators in the Middle East and North Africa (MENA) have seen their open banking upgrades put to the test in recent months as many of these countries rolled out such laws only within the past couple of years. The Central Bank of Bahrain supported the launch of the region's first open banking financial product in 2019, for example. Saudi Arabia's FinTech ecosystem has meanwhile seen steady growth as its financial officials issue more licenses enabling companies to work on banking proofs of concept. Recent reports have stated that approximately 60 FinTechs are now operating within its borders — just 20 were active in 2019.

Many of these regulators took their initial open banking cues from the General Data Protection Regulation (GDPR) and the revised Payment Services Directive (PSD2), which were both enacted by the European Union and United Kingdom in 2018. This means that MENA lawmakers are now dealing with the same pandemic-driven stressors as their international contemporaries, however. They must work to support a sizable share of consumers and merchants that are flocking to digital channels — and rapidly changing their views on the attached security standards.

Many consumers do not plan to revert into their prepandemic shopping habits once the health crisis abates, either, with 40 percent of United States consumers in a recent PYMNTS report claiming they

planned to maintain their newfound digital ways. This means regulators worldwide must carefully consider how their emerging regulations will fare in the current digital ecosystem.

AROUND THE DATA PROTECTION WORLD

The pandemic is likely to put Egypt's nascent data privacy regulations to the test sooner rather than later. The nation's data protection law officially went into effect in July, and regulators are giving banks and businesses until mid-October to become fully compliant. The regulation aims to grant Egyptian residents similar data protections and privacy standards to the ones given to EU individuals under GDPR, a partial inspiration for the new law. Egypt's regulation comes as its financial authorities attempt to establish the country as a hub for digital commerce and activity.

Consumers' payment preferences have also shifted dramatically during the pandemic, prompting merchants to explore methods that can cater to consumers' new desires while complying with existing regulations. One recent report found that 90 percent of consumers in the United Arab Emirates would switch to purchasing from merchants that supported contactless payments, for example. UAE retailers are well aware of touchless payments' growing popularity, but offering these payment

methods requires keeping them secure and ensuring they adhere to relevant regulatory standards.

Regulators in the EU and the U.K. are also struggling with the pandemic's impact on digital banking. Only 35 percent of professionals in one recent study stated that their companies were meeting all GDPR requirements, for example. Noncompliance with the regulation can be costly for firms and can erode users' trust, which is crucial to successfully maintaining business operations as eCommerce gains primacy. This issue is also noteworthy because GDPR is often cited as a blueprint for similar rules in other markets, meaning stumbling blocks regarding the regulation could appear elsewhere.

For more on these stories and other global data and payment regulation headlines, check out the Guide's News and Trends section (p. 13).

WHY PANDEMIC-DRIVEN ONLINE PAYMENT SPIKES ARE PUSHING MIDDLE EASTERN REGULATORS TO CONFRONT PRIVACY QUESTIONS

The ongoing COVID-19 pandemic has affected banking and commerce in the Middle East much as it has in other regions, pushing these activities online for many consumers. This behavior will likely continue even after the pandemic has dissipated as more customers grow familiar and comfortable with digital payments, but it also means Mideast regulators must reevaluate how they treat digital transactions as well as the data attached to them. Many of these nations' data privacy and security rules have not been updated in decades, which could open up their digital markets — and the merchants selling on them — to fraud. In this month's Feature Story (p. 8), Oren Paran managing director for Israeli retail start-up firm Retail Innovation Club and David Macadam, CEO of retail consortium The Middle East Council of Shopping Centres & Retailers (MESC), examine how the pandemic has pushed payments online, what this push means for online payment and privacy standards and why merchants need to pay attention to potential regulatory shifts.

DEEP DIVE: HOW CONSUMERS' CHANGING PAYMENT PREFERENCES ARE AFFECTING MENA PRIVACY LAWS

Consumers in the MENA region have been flocking to online channels since the pandemic's onset and businesses have followed suit by deploying new digital payment capabilities and offerings. This digital shift is leading consumers to examine just how private their online activities are, with one recent survey finding that 84 percent of UAE consumers have tried to remove private information from websites or social media. Questions regarding data privacy regulations are expanding in scope and scale as regulators take careful note of consumers' concerns. This month's Deep Dive (p. 19) investigates how the health crisis is changing MENA consumers' long-term payment preferences and explains how these shifts will affect the future of the region's open banking and privacy regulations.

5 FIVE FAST FACTS

44%

Share of UAE businesses adopting contactless payments for the first time during the ongoing pandemic

56%

Portion of U.S. consumers who now view fraud protection as more important than privacy when shopping online

26%

Portion of professionals who are unsure of their companies' GDPR compliance

80%

Share of UAE IT professionals who believe storing sensitive data in-market is either "somewhat" or "critically important"

48%

Portion of UAE SMBs that stated online data security and privacy was their top priority

HOW MIDDLE EASTERN MERCHANTS CAN KEEP UP WITH

PANDEMIC-DRIVEN PRIVACY, PAYMENT SHIFTS

FEATURE STORY

Consumers around the globe have moved their purchasing online during the COVID-19 pandemic, and those in the MENA region are no exception. The region's FIs and merchants have needed to work swiftly to support unprecedented levels of digital payment and shopping growth.

The true change merchants are facing is not in trying to stay on top of a spike in online users. Consumers have been steadily moving to eCommerce and online banking platforms for almost a decade, after all. What has shifted most during the pandemic are consumers' views on the data privacy and online security standards attached to these digital transac-tions, Oren Paran, managing director for Israeli retail startup firm Retail Innovation Club, explained in a recent interview with PYMNTS.

"People were very careful about security and privacy," Paran said. "I think the pandemic lowered this level because [many] more people are now using online shopping than they did before."

The historic wariness regarding online transactions has continued to dissipate rapidly over the past few months, David Macadam, CEO of retail consortium MESC, said in a separate PYMNTS interview. This does not mean that consumers' online data privacy and security concerns do not remain high, he stated, but that the impetus is now on the merchants facilitating digital transactions to meet consumers' cybersecurity expectations. Regulators are also looking more closely at the authentication measures attached to online payments as they continue to jump in volume, meaning merchants must keep pace with new compliance requirements as well as shifting consumer perceptions.

ONLINE PAYMENTS DRIVE PRIVACY CONCERNS

Middle Eastern consumers' jump to online channels during the pandemic follows global commerce and banking trends, but Macadam explained that the region's shift has been more dramatic than in other areas. He noted that online shopping's market penetration was hovering at roughly 3 percent to 4 percent prior to the pandemic, but it is now around 6 percent. Consumers are also beginning to adopt new payment methods, eschewing cash for debit cards, credit cards or mobile wallets that can be used for brick-and-mortar as well as online transactions.

"This region, I think, has adopted the use of credit cards much more strongly in the last six months than it has in the last five years," Macadam said.

Paran said that this type of growth can also be seen in Israel, with consumers exploring alternative payment methods like mobile wallets or touchless payments that can minimize physical contact at brick-and-mortar stores. This is also a significant departure from the pre-pandemic payment normal, he stated.

"The majority of the physical stores are still operating and looking for ways to minimize physical contact and [to] transfer the user experience to be-come as seamless as possible," Paran said. "One of the main interaction points [is] the checkout, where we are seeing a surge in contactless payments, [a method that] is still very premature in Israel compared with other markets worldwide."

This region, I think, has adopted the use of credit cards much more strongly in the last six months than it has in the last five years.

These large-scale shifts in consumers' preferences and capabilities regarding payments and bank account access have therefore prompted many to view online banking and payments with greater scrutiny. They also illustrate the dangers that can befall consumers and merchants alike when pandemic-driven

online usage outstrips current rules. Israeli lawmakers have not made significant upgrades to the country's data privacy law since 1981, for example, which could open the market to more fraud as its merchants race to support multiple payment methods on various channels.

"It is definitely getting more and more clear that [merchants] need to [support] several [payment methods]," Paran said. "You need to open your gateway to every possible transaction [type] that someone has decided they want to do."

Other regulators are working to keep pace with a pandemic-driven focus on online privacy standards. Officials in Dubai recently revamped their regulations to ease merchants' payment frustrations and to keep consumers' transactions seamless and secure. The nation's rule sets new standards for online entities' treatment and storage of digital data that largely mirror those in the EU and U.K. under the

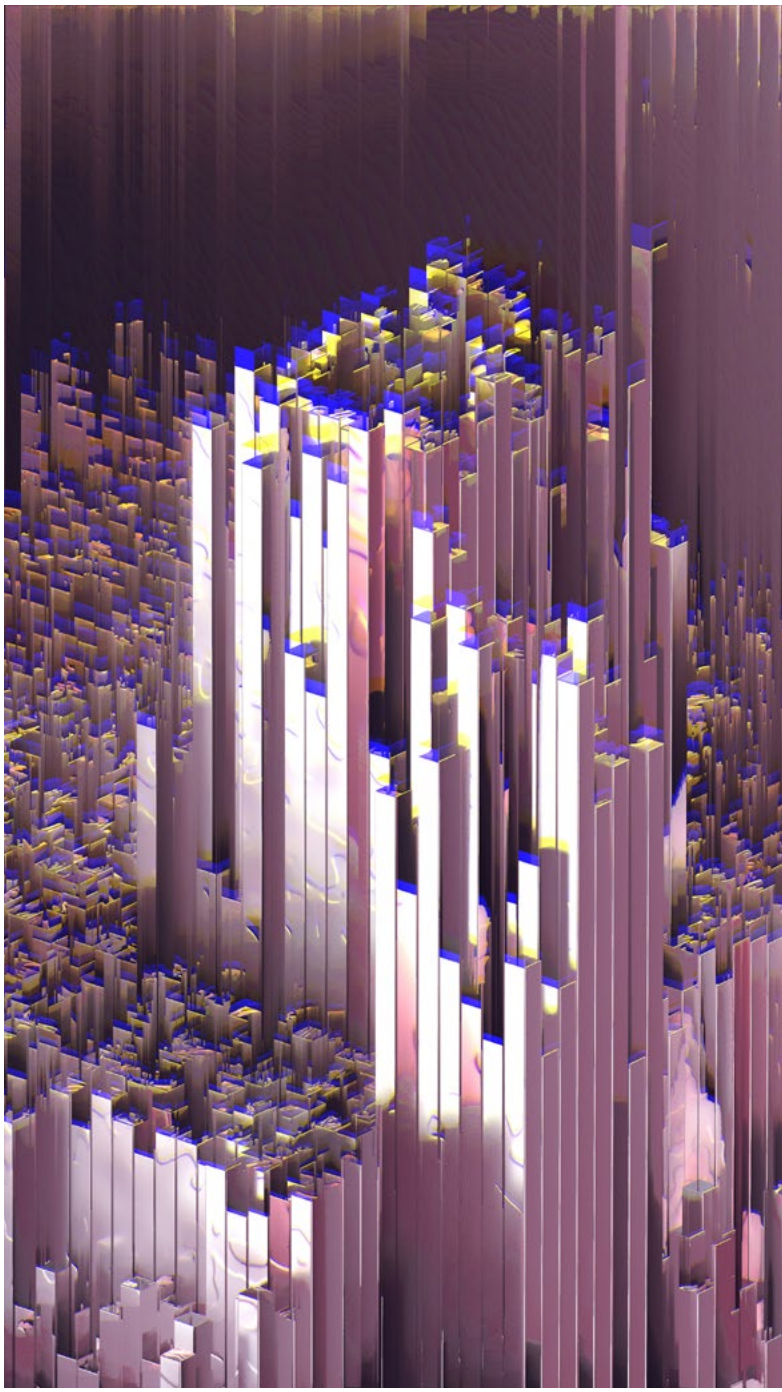
GDPR. Dubai's merchants will now be expected to more strictly safeguard much of their customers' information, and this is likely to occur within many other Middle Eastern countries in the near future.

JOINING THE GLOBAL OPEN BANKING PUSH

Regulators in the UAE and Saudi Arabia are also looking at online data protections in their markets, with these countries' merchants waiting to see how any shifts will change consumer interactions and payment data acceptance. This means Middle Eastern merchants — as well as those operating worldwide — should brace for long-term, systemic shifts in commerce and payments. Doing so successfully will rely on how knowledgeable their payment partners are, Macadam advised.

"I think it is up to the credit card companies to pay attention to the retailers and help everyone understand what is best for them," Macadam said.

Making sure merchants are well-advised and ready to confront upcoming open banking changes is critical as the pandemic pushes these developments to the next level in numerous global markets. Merchants, their payment providers and their regulators must keep up.



NEWS & TRENDS

MENA OPEN BANKING DEVELOPMENTS

EGYPTIAN BUSINESSES, FIs GEAR UP FOR NEW PRIVACY LAW

Egypt's merchants are bracing for changes affecting how they can store and utilize customers' personal information as they prepare for the country's upcoming data protection law. The Data Protection Law, which was announced last year and officially ratified this July, was crafted to give the nation's businesses guidelines for online data processing and storage. It also codifies privacy standards and rights for Egyptian individuals similar to those that were granted to EU residents under GDPR, penalizing companies that do not meet these mandates. The country's lawmakers are giving businesses and FIs until Oct. 15 to adapt their systems to achieve compliance.

The Egyptian law — unlike the GDPR — concerns only electronic data rather than all sensitive information regardless of how it is sent, processed or stored. This is partly because Egypt's rule aims to foster digital banking and commerce within the country as having dedicated online privacy standards may help it become a digital hub.

SAUDI ARABIA FINTECH ECOSYSTEM MAINTAINS PACE OF EXPANSION

Regulators in Saudi Arabia, which has witnessed steady growth in its FinTech ecosystem for the past several years, are also aiming to support digital expansion. A startup initiative called FinTech Saudi recently reported that more than 60 FinTechs are operating within the country — a considerable increase from the 20 companies that set up shop there in 2019. Approximately 100 FinTech startups are conducting proofs of concept ahead of their official market launches, according to FinTech Saudi.

Some of the growth can also be attributed to regulatory agencies' increased participation, according to the initiative. The Saudi Arabia Monetary Authority (SAMA) and Capital Markets Authority (CMA) have begun to grant regulatory permits for these proofs

of concept as well as other tests required to develop digital banking products. FinTech Saudi said the industry would be unlikely to sustain its current growth without the issuance of such permits.

CONTACTLESS PAYMENT ADOPTION ON THE RISE IN UAE

The pandemic is also rapidly changing how consumers in various markets shop and pay, leaving banks and merchants scrambling to keep up with digital trends. One recent study found that 90 percent of UAE customers would switch to making purchases from merchants that supported contactless payments, for example. Retailers are also working to enable touchless payment options to keep customers satisfied as 94 percent of the country's small to mid-sized businesses (SMBs) say they have integrated contactless payments into their point-of-sale (POS) systems since the pandemic began. Forty-four percent of these businesses are utilizing contactless payments for the first time, in fact.

UAE consumers and merchants are ahead of the curve in adopting contactless methods: The share of the nation's businesses that accept such payments is more than double the global median.

PAYMENT UPGRADES AND ONLINE REGULATIONS

MERCHANTS EXAMINE 3D SECURE 2.0, OTHER SECURITY TOOLS AS CONTACTLESS PAYMENT USE GROWS

American shoppers are also more frequently tapping contactless and mobile payments during the pandemic, with one payment service provider's recent card data showing that mobile wallet-enabled debit transactions rose by 76.6 percent year over year during the week of Aug. 9. This growth is prompting merchants and their payment providers to reexamine the security measures attached to card-not-present (CNP) payments. 3D Secure 2.0 software, which encrypts payment details to provide

enhanced fraud protection for consumers and merchants, has sparked increased interest.

Retailers must ensure that such security technologies do not add too much friction into the online payment experience as consumers tend to abandon purchases that frustrate them. This concern is becoming especially familiar to merchants in the EU and the U.K. working to craft identity verification tools that can satisfy customers while complying with upcoming strong customer authentication (SCA) mandates.

US CONSUMERS EYE eCOMMERCE SECURITY STANDARDS

Consumers in the U.S. are also changing their online security perceptions. One recent survey found that 56 percent of U.S. individuals shopping online see fraud protection measures as more important than the privacy standards attached to their payments, for example, while 92 percent stated that they felt security was critical when making online purchases.

Consumers have mixed opinions regarding which party is responsible for providing cybersecurity, however. About one-third of shoppers said that individual retailers or websites should be in charge of providing fraud protection measures while 23 percent said it was the responsibility of merchants' banks or payment partners. Certain states are also generating their own rules and a dedicated federal policy for the transmission of online payments or information has yet to emerge. Promoting comprehensive online security processes and making them more transparent for consumers could resolve some confusion.

CALIFORNIA LAWMAKERS AIM TO CUT OFF PREDATORY SMB LENDING PRACTICES

Legislators in California have been busy ratifying several online finance and data privacy regulations, including the California Consumer Privacy Act (CCPA), which grants its residents digital data protections. The state's lawmakers recently passed another bill that will expand the jurisdiction of its Department of Business Oversight and rename it the Department of Financial Protection and Innovation (DFPI). The bill will enable the agency to charge companies for unfair and deceptive policies or other forms of misconduct, which could significantly alter how California approves and regulates SMB loans.

This switch affects lending in particular because it places nonbank SMB lenders under the department's purview for the first time. These lenders were not previously regulated to the same standard as their bank counterparts, meaning the legislature grants another protective layer to California SMBs seeking funding. Approximately 4 million SMBs are active in the state.

SECURITY AND DATA PRIVACY

CONFRONTING THE COST OF DATA BREACHES IN THE MIDDLE EAST

Banks and companies in the Middle East remain popular targets for fraudsters, making robust cybersecurity measures a top concern for these entities. A recent report revealed that the price of data breaches in countries like Saudi Arabia and the UAE is on the rise, growing by 9.4 percent from 2019, for example. Hacks now cost such companies an average of $6.53 million, compared to the global average of $3.86 million.

The report also examined some of the factors that could be contributing to this higher cost, including the speed at which companies can respond to data breaches and other fraudulent activity. Saudi Arabian and UAE companies have managed to reduce the time it takes to identify a data breach by 10 days compared to last year but the study found that it still takes them 269 days on average to isolate fraud events.

COMPANIES WORLDWIDE REPORT CONTINUING DATA PRIVACY STRUGGLES

Regulators in some markets are prioritizing privacy-related efforts as well as security measures, but many of these initiatives are still facing hurdles. GDPR, which governs data privacy in the EU and the U.K., went into effect in May 2018, but merchants in these markets still report compliance challenges. One recent study found that just 35 percent of professionals said their businesses were meeting all GDPR mandates while 26 percent were unsure if

their companies' policies were fully compliant with the regulation.

British and EU firms are not alone in their confusion regarding online privacy compliance. The survey also revealed that 28 percent of California's merchants were unsure whether their privacy policies complied with the CCPA, and 14 percent of the state's merchants stated they were currently not compliant. This indicates that businesses of all stripes are searching for more transparency when it comes to such rules.

TECH FIRMS COME UNDER GDPR FIRE

Businesses of all sizes are still adjusting to GDPR-related changes, with technology providers Oracle and Salesforce recently experiencing extra regulatory scrutiny, for example. The Privacy Collective, a nonprofit Dutch consumer privacy advocacy group, has alleged that the firms' online data policies do not comply with GDPR, and the group intends to file suit in courts in the Netherlands and the United Kingdom. The case would represent the Netherlands' largest-ever class-action GDPR lawsuit, according to reports.

The allegations state that both companies are engaging in a process known as "real-time bidding," in which consumers' information is marketed and sold to third-party companies without their knowledge. This typically begins with businesses adding cookies on users' devices that track their activities, and the Privacy Collective is also claiming the way that Oracle and Salesforce trace such cookies is noncompliant with GDPR. The two firms could face collective penalties of about €10 billion ($11.5 billion USD).

INTERNATIONAL PRIVACY, REGULATORY CHALLENGES

EU AUTHORITIES PUSH FOR INTERNATIONAL DATA PRIVACY STANDARDS

Some companies are struggling with regulatory compliance issues due to the disparity between the EU's standards and those in other countries and regions, but the development of international data privacy rules could solve such problems. Two EU regulatory figures — Alessandra Pierucci, the chair of the Council of Europe's data protection committee, and Jean-Philippe Walter, its data protection commissioner — are both calling for such standards to achieve this.

The two are proposing that more countries adopt "Convention 108," a rule the council developed in 1981 that has been upgraded to reflect today's digital banking and commerce atmosphere. They argue that doing so would offer countries a starting point that would enable them to craft their own data privacy and protection initiatives. Fifty-five countries have thus far adopted the measure.

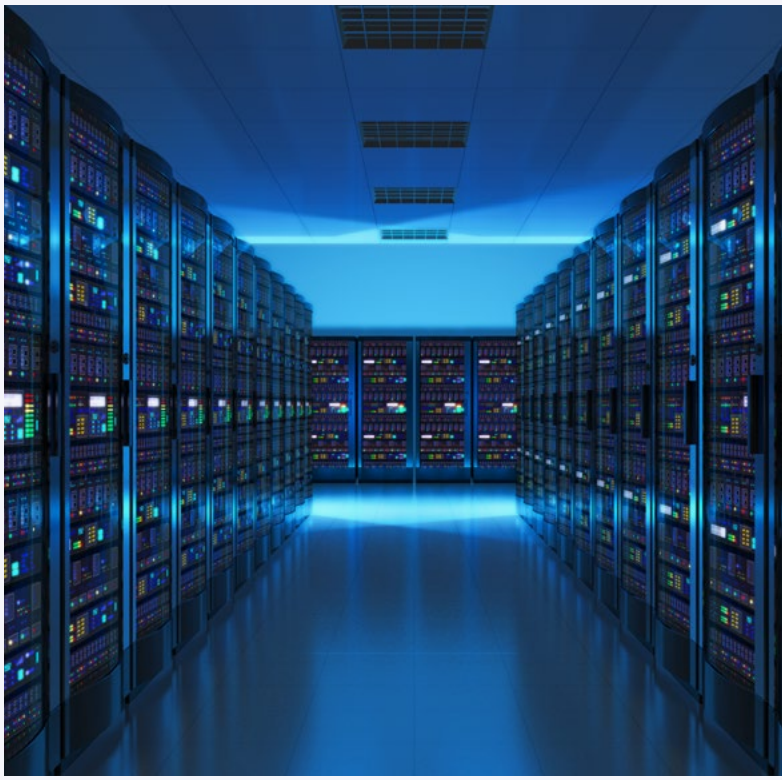
EU, US REGULATORS SETTLE IN FOR PRIVACY SHIELD BATTLE

Determining where sensitive data can be stored is another key issue when creating international privacy regulations, prompting an EU court to strike down the Privacy Shield framework that had been set up to enable data transfers between companies in the U.S and the EU. The court highlighted the differences between the two markets' privacy standards, with some members arguing that EU consumers' personal information was not fully protected when stored on U.S.-based servers. The decision presents a significant challenge to many American companies that wish to continue doing business in the EU.

Storing such information on servers in the EU presents one potential solution for U.S. companies, but such a move is not feasible for all businesses. Regulators from both the EU Commission and the U.S. Department of Commerce are thus working on a compromise by upgrading the Privacy Shield, but the process will likely take at least several years.

CHINA GEARS UP FOR A DATA SECURITY PUSH

China is also joining in the international debate over security standards. The country's foreign minister recently unveiled a plan called the Global Initiative on Data Security, which proposes comprehensive cybersecurity guidelines that can enable countries to send data through secure channels. The proposal comes as China and the U.S. face off on data



security-related concerns, with the American government pointing to potential security weaknesses and threats attached to Chinese-owned social applications and technology firms. Chinese officials have meanwhile stated that the U.S. is applying double standards to digital privacy that put China's companies at a competitive disadvantage in the technology market.

DEEP
DIVE

Why The Pandemic Is Pushing MENA Regulators To **Upgrade Open Banking, Privacy Laws**

Consumers and businesses have been moving online in recent years, and regulators from the EU to the MENA region have worked to keep up with this migration. The ongoing COVID-19 pandemic is accelerating this shift, making FIs, merchants and their regulatory officials race to secure these new digital users.

The health crisis is prompting officials to adjust their views on financial regulations as many authorities had different priorities when they passed the first iterations of such rules more than a decade ago. The Dubai International Financial Centre ratified the original version of its Data Protection Law (DPL) in 2007, for example — about a year earlier than Europe's official GDPR and first PSD launches. Financial authorities and lawmakers in Abu Dhabi, Saudi Arabia and the UAE quickly followed Dubai's lead as consumers and merchants headed online.

MENA nations' original rules involved data privacy, but they were focused on developing the open banking ecosystem and allowing information to move freely. The pandemic is dramatically altering how merchants can transact, which data they can store and where they can store it, however. Regulators as well as finance and technology experts are scrutinizing where digital information is held, and one recent survey found that eight out of 10 IT professionals in the UAE believe storing sensitive information locally is either "somewhat" or "very important."

The following Deep Dive analyzes how the pandemic has affected open banking and privacy regulations — especially in the MENA region — and implicated future regulations. It will also examine how merchants

can better understand these rules and compete within an ecosystem where online privacy and digital banking perceptions are shifting.

THE DATA PRIVACY TWIST

Cybersecurity and data privacy have always been critical facets of open banking regulations as fraud tends to increase alongside growing online transaction volumes. Data breaches now cost Saudi Arabia and UAE companies about $188 for each stolen personal detail, for example, and this price tag is exponential because most hacks compromise thousands of records. The pandemic has refocused scrutiny on the open banking ecosystem's privacy and security.

Part of the reason for this new spotlight on data privacy is simple: MENA consumers are starting to question how their data will be used and where it will be stored. A May 2020 survey of UAE consumers found that 84 percent tried to remove private details from online websites or their social media, for example, and 31 percent stated that their personal data had been shared or made available to others without their explicit consent. These views are significant for merchants and regulators because most of these consumers expect to maintain their digital

habits after the pandemic ends. Sixty-nine percent of MENA consumers believe the health crisis will significantly alter their long-term behaviors while just 9 percent expect to return to their prepandemic spending habits once the pandemic abates.

Consumers' changing views are prompting MENA financial authorities to reexamine how their present regulations handle online privacy. Egypt recently announced that its first consumer-related data protection rule would go into effect in October, for example, and the Dubai International Financial Centre (DIFC) revealed in July that it was upgrading its DPL, with businesses given until Oct. 1 to adjust their standards in compliance. This shift has been pushed further into the spotlight due to the ongoing pandemic. Dubai's rule contains greater financial penalties for organizations that fail to comply, indicating that its newfound data privacy focus is likely a long-term priority. Lawmakers in Abu Dhabi have also amended existing rules during the pandemic — a move that could radically shift open banking developments.

MERCHANTS AND THE GLOBAL PRIVACY BATTLE

Perhaps the most notable detail about the MENA region's developing open banking standards is their scope. Dubai's regulation covers all businesses that are keeping or employing individual residents' data, making its reach similar to that of the GDPR and the CCPA in their respective markets. The comprehensive nature of these regulations could prove crucial to businesses, as one study found that online privacy and security was a main worry for 48 percent of SMBs in the UAE, for example.

These standards may provide additional layers of security that are likely to please consumers, but they could also put merchants in a precarious position as they look to adhere to domestic and international privacy regulations. Many merchants are global entities, after all, which means they must now worry about security regulations in their own markets and abroad.

Businesses must therefore keep a careful eye on how data privacy perceptions are changing worldwide, especially as the pandemic pushes more regulators into action. Regulators must also consider the increasingly global nature of commerce and finance to craft security standards that can satisfy businesses, banks and customers. The development of an international data privacy standard may be years away, but developing cohesive regulatory policies for open banking is becoming more and more essential for businesses in the MENA region and beyond.

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 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.

EKATA

Ekata is an international identity data company that provides businesses with global identity verification solutions via enterprise-scale APIs and web tools to help companies identify legitimate customers, prevent fraudulent transactions, and smooth new customer creation. Ekata services customers from offices in Singapore, Budapest, Amsterdam and Seattle.

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 feedback@pymnts.com.

DISCLAIMER

The Merchants Guide To Navigating Global Payments Regulations 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.