DEFINING NEW CUSTOMER JOURNEYS

Payment Services Directive 2 (PSD2) Scoping out the impacts of the Regulatory Technical Standards (RTS) on Strong Customer Authentication and Common and Secure Open Standards of Communication

Assessing the EC's final Regulatory Technical Standards (RTS) published in the Official Journal of the European Union on 13th March, 2018 and their effects on payments use cases and business models.

An Accenture Point of View paper

accenture

CONTENTS

INTRODUCTION

The introduction of the revised Payment Services Directive (PSD2) is a defining moment for banks in Europe. It is a data and technology-driven directive that aims to create increased competition, innovation and transparency across the European payments market, while also enhancing the security of Internet payments and account access.

In pursuing these aims, the directive is set to accelerate the digital disruption that is reshaping the financial services industry. It will do this by bringing new forms of payment institutions within the scope of regulation, introducing new interaction models, and mandating that banks open up their systems to third parties through interfaces such as open application programming interfaces (APIs). At the core of PSD2 is a requirement for banks to grant third-party providers (TPPs) access to their customers' online accounts and payment services in a regulated and secure way.

A CRITICAL JUNCTURE IN THE TIMELINE...

While the whole PSD2 initiative represents a major change for banks, we are currently at an especially critical juncture in the timeline for its introduction. On 13th March, 2018 Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC) under PSD2, were published in the Official journal of the European Union, binding them into EU law, for transposition by member states. The RTS were first drafted by the European Banking Authority (EBA) in 2016 and have undergone several iterations with the EBA and European Commission, and banks and other payment services providers (PSP) have to comply with them from 14th September, 2019. The finalization of these RTS has been a difficult process. Multiple interest groups in the European financial services industry discussed the impact of the RTS on existing use cases and business models, and lobbied in favor of their own preferences. The key area of contention was the use of screen scraping, which was demanded by the Fintech industry where it is in regular use, but was resisted by banking associations, which view screen scraping as insecure.

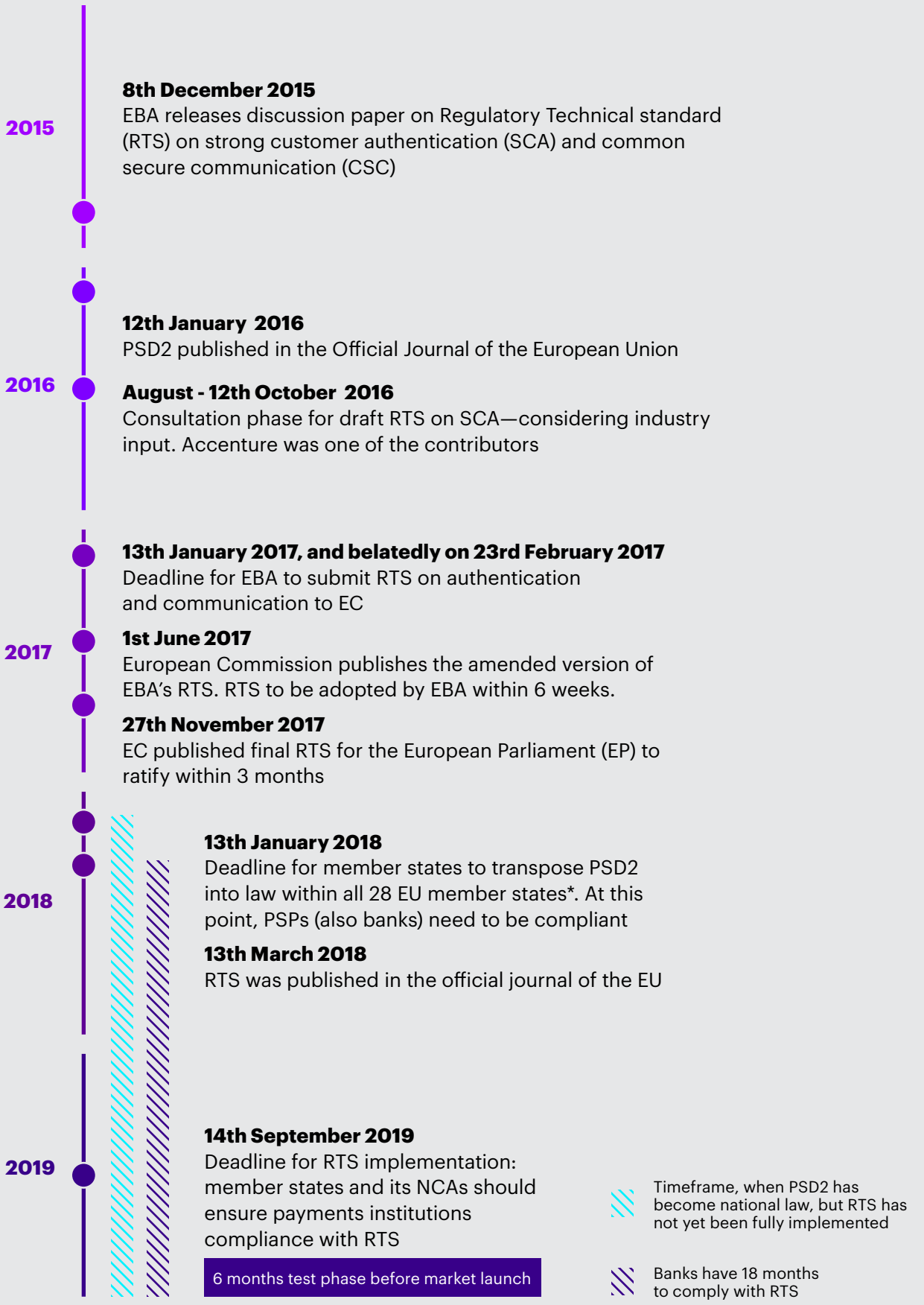
The following are the main points clarified and finalized in the RTS:

Dedicated APIs are a choice not an obligation for banks, the alternative being to rely on "TPP-authenticated" user-facing screen scraping technology on their normal customer interface (online or mobile banking)

Banks choosing dedicated APIs still need to provide screen scraping as a fallback solution. Exemption from fallback can be granted by a bank's National Competent Authority (NCA), after proving properly-tested, performant and available dedicated APIs six months before market launch

The actual service level requirements on API performance and availability are currently defined by the API Evaluation Group of the European Retail Payments Board (ERPB)

The permitting of contingency measures, including "screen scarping" in cases where the dedicated APIs are unavailable five consecutive times for more than 30 seconds or have performance issues.


2015
8th December 2015
EBA releases discussion paper on Regulatory Technical standard (RTS) on strong customer authentication (SCA) and common secure communication (CSC)
2016
12th January 2016
PSD2 published in the Official Journal of the European Union
August - 12th October 2016
Consultation phase for draft RTS on SCA—considering industry input. Accenture was one of the contributors
2017
13th January 2017, and belatedly on 23rd February 2017
Deadline for EBA to submit RTS on authentication and communication to EC
1st June 2017
European Commission publishes the amended version of EBA's RTS. RTS to be adopted by EBA within 6 weeks.
27th November 2017
EC published final RTS for the European Parliament (EP) to ratify within 3 months
2018
13th January 2018
Deadline for member states to transpose PSD2 into law within all 28 EU member states*. At this point, PSPs (also banks) need to be compliant
13th March 2018
RTS was published in the official journal of the EU
2019
14th September 2019
Deadline for RTS implementation: member states and its NCAs should ensure payments institutions compliance with RTS
6 months test phase before market launch
Timeframe, when PSD2 has become national law, but RTS has not yet been fully implemented
Banks have 18 months to comply with RTS
* Netherlands announced a delay of implementing PSD2 into national law (estimated in spring 2018)

...AS A GAP OPENS UP BETWEEN PSD2 AND THE RTS

With PSD2 having been introduced on 13 January 2018, it was inevitable even the iterations to refine the RTS, would open up a timelag between the point where banks had to be PSD2 compliant, and the deadline for them to comply with the additional RTS. In the transition period after PSD2 became national law in January 2018 and the point where the RTS become effective from 14th September 2019, banks must allow unrestricted access by third parties via their existing interfaces until they have new PSD2 RTS compliant ones in place.

In 2017, banks faced a difficult choice about whether to press ahead with work to achieve PSD2 compliance, or hold off until the RTS were approved. Now that they know the RTS requirements with certainty, they need to act. If they have waited for the final RTS, they should take steps now to provide dedicated APIs with or without fallback, or to rely on screen scraping of the customer-facing interface only.

PSD2 is technology-neutral, and banks can get by from January 2018 without publishing APIs by allowing AISPs and PISPs to screen scrape their online accounts, without contractual agreements. Banks can leave implementing API or authenticated screen scraping solutions until 14th September, 2019. Even so, banks should be compliant now with all articles of the PSD2, except for some provisions within some of the articles related to security and the RTS. Specifically, the application of Articles 65, 66, 67 and 97 of PSD2 has been postponed until 14th September, 2019. However, those parts of Articles 65, 66, 67 and 97 that are not dependent on the RTS have been in force since 13th January 2018. PSPs should also use the period up to 14th September 2019 to upgrade their payments security systems to meet the RTS requirements.

A TIME TO CREATE FRICTIONLESS, SECURE SOLUTIONS

Accenture's view is that the gap between PSD2 and the RTS ultimately makes no difference to the need to be compliant. What's more, banks should now be focusing on creating solutions that enable a frictionless customer experience supported by slick, unintrusive customer authentication using advanced tools such as behavioral biometrics. Equally importantly, these solutions must be secure to ensure the level of fraud committed on transactions conducted through them is low.

By developing such solutions, banks will be fully aligned with one of the European Commission's key high-level objectives with PSD2—which is to bear down on the alarming growth in fraud in online payments such as card-not-present transactions. If banks' solutions are secure against fraud, then they can be sure they will be in line with the intent of the RTS whenever they come into force, while also meeting the exemption criteria applied under PSD2 for low levels of fraud.

In Accenture's view, the way forward for banks and other PSPs is clear. While the time gap between PSD2 and the RTS enforcement presents an issue, one workable solution is to focus on delivering the outcome targeted by both of these sets of regulations: a frictionless customer experience with very low levels of fraud. Develop a solution to deliver these attributes, and compliance should follow naturally from there.And while screen scraping may appeal to smaller banks with limited resources, for those banks that want to participate in the API economy, keep competitive and exploit the benefits of Open Banking, open APIs are the way to go.

KEY ASPECTS OF THE FINAL EC RTS

BANKS' OBLIGATIONS AND SERVICES TO AISPS AND PISPS

Compared with the initial draft RTS published in 2016, and the EC's amendments to EBA's final draft in June 2017, the EC's final RTS contain a number of key changes and additions. Importantly, the final version clarifies banks' obligations and service provision to AISPs (Account Information Service Providers) and PISPs (Payment Initiation Service Providers). These clarifications include detailed definitions of the functional and technical rules of the "dedicated interface" (API), on SCA, including application and exemptions; and on secure communication between third-party payment service provider (TPPs) and banks.

Here are the aspects of the final RTS that are most likely to have an impact on existing use cases, and to open up opportunities for new ones.

OPEN APIS FOR AISPS AND PISPS

According to the final RTS, banks with payment accounts that are accessible online must offer at least one interface enabling secure communication with AISPs for account information, and with PISPs and PSPICBPIs (payments service providers issuing card based payments instruments) for payment initiation. Banks have to grant authorized AISPs access to the same account information as provided to the bank's own services—including transaction history—at the same cost to the account holder, typically free of charge for consumers. They must also grant authorized PISPs access to the same payment instruments as provided to the bank's own services, again at the same cost, typically free of charge for consumers.

Further provisions include a right for PISPs to communicate with banks to receive information on the initiation and execution of payment transactions, and a requirement for banks to provide PISPs immediately with the same level of information they give to users. As per the European Commission's changes to the RTS, accessing accounts through screen-scraping as a fallback solution—technology that enables TPPs to access a customer's bank accounts on their behalf using the customer's own access credentials—is allowed when the dedicated API is unavailable for more than 30 seconds or is suffering from inadequate performance. But banks can be exempted from offering the fallback solution by the NCA if they passed a six-month testing period with the market and prove highly available and performant APIs. Finally, while the EBA requirement for financial messaging format

ISO20022 for dedicated interfaces has still been left out of the EC's final text, it is prudent to build APIs using state-of-the-art RESTful design methodologies and formats such as JSON with ISO20022 elements, as it is a widely-used standard. The Open Banking Standard in the UK is an example of using JSON and ISO20022 elements, and the Berlin Group's NextGenPSD2 standard also relies on JSON.

STRONG CUSTOMER AUTHENTICATION (SCA)

To qualify as SCA for authorizing transactions, the SCA process will have to apply at least two of the three key authentication elements of knowledge, possession, and inherence. PISPs and AISPs will have the right to rely on authentication methods such as smsTAN (such as authentication codes received on SIM-based mobile phone) and chipTAN (a separate security device) provided by banks to the Payment Service User (PSU). In these latter cases, the authentication method will fully remain within the sphere of bank's competence.

AISPs can request account information up to four times a day after an initial SCA—unless they have a bilateral agreement in place with the bank—and at any time when the PSU is actively requesting account information. The user must give consent for every payment initiation and account information request, as a general mandate for designated payment accounts.

SCA CRITERIA

The final RTS state that the following criteria will be applied in assessing whether authentication methods qualify as SCA:

DYNAMIC LINKING: The authentication code generated through the SCA needs to be specifically linked both with the amount paid and the payment recipient, and must be shown to the payer. Also, all information about the amount paid and the payment recipient must be passed on across all phases of the authentication—generation, transmission and application—and shown to the payer.

INDEPENDENCE OF CHANNELS: The channel that is used for the initiation of a payment or account information transaction must be separate from the channel used for the reception of the authentication code. Multi-purpose devices such as smartphones can be used for more than one of the authentication elements, provided separate execution environments on the device are used for the different elements, and that there is a mechanism to ensure the device or software is not altered by the payer or TPP.

IDENTITY CHECKING WITHIN THE BANK'S ENVIRONMENT: Identity checking of the PSU—involving the association of the user's identity with personalized security credentials—is the bank's responsibility, and needs to take place within the bank's environment. Identity checking via a remote channel requires SCA.

UNDERIVABLE AUTHENTICATION CODES: Authentication codes must not give any indication about the other authentication elements and their mechanisms. Also, it must not be possible to derive or forge codes from previously created ones.

NON-DISCLOSURE: Security credentials must not be stored in plain text, and the related secret cryptographic materials must be protected from unauthorized disclosure.

AN ASSESSMENT OF EXISTING AUTHENTICATION METHODS AGAINST THE RTS REQUIREMENTS

The table below shows an assessment of the most widespread existing authentication methods used in Europe against the SCA criteria set out in the RTS.

AUTHENTICATION METHOD*	DYNAMIC LINKING	INDEPENDENCE OF CHANNELS	BANK ENVIRONMENT	UNDERIVABLE AUTHENTICATION CODES	NON-DISCLOSURE
iTAN (list of printed indexed Authentication codes)	X	✓	X	✓	X
smsTAN (Authentication code is sent to a GSM mobile number)	✓	X	X	✓	✓
photoTAN (Authentication code is sent as a graphic picture on a secure smartphone app)	✓	X	✓	✓	✓
chipTAN (Authentication code is generated on a separate security device with a smartcard and PIN)	✓	✓	✓	✓	✓
BestSign Touch ID (Authentication performed via Apple's Touch ID)	✓	X	X	X	X
BestSign Dongle (Authentication code is generated on a separate security device using Bluetooth and PIN)	✓	✓	✓	✓	✓

*TAN stands for 'transaction number', and is equivalent to 'authentication code'

As the table illustrates, the current version of the RTS does not allow for today's most user-convenient authentication methods. Currently, the only RTS-compliant technologies are those that require a separate security device. Since authentication methods using a separate security device are not convenient for users, banks need to develop innovative, secure and convenient authentication methods (such as biometrics) using multi-purpose devices. This will become a major competitive factor for banks.

EXEMPTIONS ALLOWED FROM SCA

The RTS allows exemptions from SCA for specific cases. These exemptions bring significant implications for some use cases and services.

PAYMENT INITIATION

RISK-BASED EXEMPTIONS

Transaction risk analysis for remote card-based and non-remote credit transfer payments

Transaction risk analysis is allowed on remote transactions to exempt them from SCA up to a maximum value of €500, provided that transaction monitoring is in place, and that fraud is kept below the Exemption Threshold Values (ETV).

ETV	REMOTE CARD-BASED PAYMENT	CREDIT TRANSFERS
iTAN	0.01	0.005
smsTAN	0.06	0.010
photoTAN	0.13	0.015

For remote card-based and non-remote credit transfer payments, banks need to use transaction monitoring to detect unauthorized or fraudulent payment transactions, with additional monitoring of exempt transactions. Factors to be monitored include previous spending patterns, transaction history, and the location of the payer and payee where the access device is provided by the bank. Banks cannot use SCA exemptions if their monitored fraud rate at the €100 ETV exceeds the threshold for two consecutive quarters.

PAYMENT CHANNEL AND INSTRUMENT-BASED EXEMPTIONS

Here are the main SCA exemptions applied to payment initiation using specific channels and instruments.

PAYMENT TYPE	SCA EXEMPTION RULE	EXAMPLES FOR PAYMENT INSTRUMENTS
Contactless electronic payment	SCA is not needed on contactless transactions below €50, or when the cumulative transactions since the last SCA are below €150 or consist of fewer than five consecutive contactless transactions.	Contactless NFC cards, NFC-based smartphones
Electronic payment at unattended payment terminals for Parking fares	PSPs are allowed not to apply SCA for payments initiated at unattended payment terminal to pay a transport fare or parking fees.	Debit/credit cards, contactless NFC cards, NFC-based smartphones
Remote electronic payment transfer	**Low Value** The low value exemption for remote transactions is €30, with a cumulative maximum total of €100 or not exceeding five consecutive transactions since the last application of SCA.	Remote credit transfer via e-banking, remote credit transfer using debit/credit cards, banking accounts, etc.
	Trusted Beneficiaries and recurring transactions • SCA is not needed where the payee is included in a list of trusted beneficiaries held by the bank, or where the payee initiates a recurring payment for the same payee and amount. • Payments of the same amount to the same payee (any payment type) are exempt.	Remote credit transfer via e-banking, remote credit transfer using credit cards, banking accounts, etc.
	Payment-to-Self SCA is not necessary when the payer and beneficiary are one and the same person and both accounts are with the same PSP.	Credit transfer via e-banking, remote credit transfer using credit cards, banking accounts, etc.
Secure corporate payment transfer	**Corporates initiating electronic payment transactions** SCA is not necessary in cases when dedicated corporate payment processes or protocols are used, provided the national competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those PSD2 aims for.	e.g., EBICS, proprietary bank interfaces

ACCOUNT INFORMATION

EXEMPTIONS FROM SCA FOR ACCOUNT INFORMATION SERVICES

For account information, banks are exempt from SCA for balance-only requests and for requests for payment transactions for a duration up to 90 days. TPPs are allowed to access this information if the customer is actively requesting. In case the customer is not actively requesting, the TPP is allowed to access no more than 4 times in a 24 hour period, unless a higher frequency is agreed between the TPP (with user's consent) and the bank.

ADDITIONAL REQUIREMENTS FOR BANKS

BANKS MUST ALSO, AMONG OTHER THINGS:

Maintain an audit trail of all PISP, AISP and PSPICBPIs requests.

Provide a testing facility for AISPs, PISPs and PSPICBPIs.

Give at least three months' notice of any change to the technical specification of their interface.

Notify the competent authorities of their intention to use transaction risk analysis.

Provide all authorized TPPs with access to their API specifications free of charge.

SOME OPEN QUESTIONS

SYNCHRONOUS CONFIRMATION

Synchronous confirmation of a successful payment does not appear to be a requirement of the RTS, but PISPs can request payment status information from the banks. The information that banks give to PISPs on initiation and execution of a payment is the same they normally give to users, but this may be insufficient for PISPs' needs. Banks typically tell users the payment is initiated successfully and should reach the beneficiary, but they don't commit to it. Payment scheme rules such as those for the SEPA Credit Transfer (SCT) scheme stipulate the requirements for successful payment completion once initiated. So provided a bank has confirmed a payment is initiated, the PISP/account holder can likely assume the bank is operating the payment in accordance with the scheme rules.

SCREEN-SCRAPING

As per the European Commission's final RTS, screen-scraping can be used as a contingency measure if the bank has availability or performance issues with the dedicated APIs as a fallback solution. In these cases, a TPP could switch from the API to the screen-scraping interface. But how does a TPP decide if the performance of the dedicated API is inadequate? And how can a bank distinguish between a TPP and an actual bank customer logging on? The Commission announced in November 2017 that it would promote the establishment of a Market Group consisting of banks, PISPs, AISPs and PSUs. This group will work on a harmonized test framework and key common requirements such as KPIs, and review the quality of dedicated APIs. This Market Group is led by the ERPB on Payment Initiation Services for API Evaluation.

SECURITY—CERTIFICATES AND EBA REGISTER

Banks need to be able to authenticate all registered TPPs and verify its validity of their license. Currently there is no available QTSPs issuing eIDAS certificates under PSD2. The ETSI is currently working on a standard for the certificates. The EBA register will include a database of all registered TPPs across the EU and updated by the NCAs. Banks need to have an up-to-date copy of the register on the bank server that can be used for an additional security check. The EBA register will not be machine-readable via tools such as APIs, and will not have a real-time notification service for status changes. The question for banks is, how can they make sure that they grant access to only registered TPPs and avoid fraud?

IMPACTS OF PSD2 AND THE RTS ON USE CASES AND BUSINESS MODELS

IMPACTS ON CARD PAYMENTS

Amid the discussion about the new market dynamics brought in by the introduction of open APIs for new payment initiation and account information services, the impacts of PSD2 and the RTS on the traditional card business seem to have been almost overlooked. However, these impacts will be substantial—and will result in major changes in the future in how customers use payment cards in almost all environments.

Impacts on POS transactions

PSD2 will have important impacts even on traditional card payments at a stationary point of sale (POS). The requirement for SCA will apply to these transactions— and as a signature will not meet the SCA criteria, signatures will have to be phased in as an authentication method in Europe during the period up to the RTS becoming law in EU member states. Because SCA is an obligation on the issuing side, issuers that are still issuing cards with a signature as the preferred CVM (customer verification method) must stop this practice and potentially replace all issued cards. However, for card usage outside Europe it will be essential not to remove the signature altogether from the CVM list. So card schemes must decide whether additional steps are needed on the acquiring side to help the issuers meet the new obligations.

The new framework for contactless transactions without cardholder verification will have an impact on the issuers and their cards. In general, the RTS allow contactless card transactions with no CVM up to a limit of €50. But the number of no-CVM transactions permitted is limited to five in a row, or a cumulative maximum of €150. Most cards do currently support a transaction counter, but do not have a counter for accumulated transaction value as this is not included in the Mastercard and Visa specifications. However, a handful of payment schemes do support this type of risk mitigation: examples include the German girocard scheme, which recently launched a contactless payments application. For most other card schemes, the need to implement the limit functions within the chip will probably require the issuance of

new cards. A further factor is that the regulators still have to decide whether the rule will apply only to cards issued after the effective date, or if all cards will have to meet these requirements after the RTS's 18-month interim period.

Impacts on card-based mobile payments

Card-based mobile payments at the POS will also be significantly affected by PSD2 and RTS since the SCA rules must also be implemented for mobile payments scenarios like HCE, Apple Pay, Samsung Pay and Android Pay. Most of these mobile applications do not yet allow for the required SCA checks, and introducing them would be a major change involving either re-designing the mobile applications themselves or implementing the checks in the issuers' authorization systems.

The requirements regarding the performance of the SCA could also pose a challenge. Some card-based mobile payment solutions do not perform the CVM by asking the cardholder to type in a PIN on the secured PIN-pad of the merchant terminals, but through a fingerprint check on the client's mobile device. These authentication methods are completely beyond the control of the card issuer and their systems, but PSD2 and the RTS put the obligation and responsibility for SCA squarely on the shoulders of the issuing bank. This means issuers must agree to hand over responsibility for the SCA to the relevant hardware manufacturer, radically changing the relationship between issuers and device makers.

Unattended POS for parking fees and transportation tickets

Under PSD2 and the RTS, customers can use electronic payment instruments such as debit/credit cards to pay for transportation tickets and parking fees without having to meet the SCA requirements. This exemption should help to boost user convenience for these common payment events in customers' everyday lives. That said, the RTS does not specify any amount limits, which could increase the risks of fraud at transportation ticket machines. It is not yet clear whether the definition of 'transportation tickets' covers only local public transport (potentially lower amounts) or longer-distance train tickets as well (potentially higher amounts).

Impacts on e-commerce transactions

Arguably the biggest impacts of the new PSD2 requirements will be in the field of remote e-commerce transactions. In general terms, card issuers will be obliged to perform an SCA check for every transaction above €30 that does not meet any of the exemption criteria. While card issuers can try to reduce the number of cases in which SCA is required, there is no way to prevent it fully. Also, merchants can no longer fend off the SCA mechanism for card payments, because the bank no longer has a free choice on whether or not to perform SCA. In cases where the issuer is required to perform an SCA the merchant must also support it, or the issuer has to reject the authorization request.

Given the rapid growth in eCommerce transactions over smartphones, issuers will need some sort of mobile app, or SMS capability, to trigger an authentication response from consumers when they use their cards online. This could be a secured environment using a fingerprint, plus a software app, or an API call to a smartphone-based banking app that asks for authentication.

For card issuers, there will be significant effort involved in implementing SCA for card-not-present payments, rolling it out, and educating their customers in how to use it. Also, it is possible that there will be different solutions for consumers depending on who they bank with, in the same way that authentication for mobile and online banking varies from bank to bank. However, EMVCo is rolling out a two-factor authentication version of 3D Secure, called 3DS 2.0, which, for example Visa is incentivizing merchants and issuers to use by April 2019. It is anticipated that 3DS 2.0 will be compatible with the EBA RTS once finalized, and could become a solution for issuers to adopt to meet their SCA obligations.

However, merchant and wallet providers remain wary of creating a situation where SCA is performed too often and disturbs the check-out process for consumers. As eCommerce grows, basket abandonment rates are a big concern for merchants. While there are various reasons for high abandonment rates, the fact remains that friction and inconvenience in the online payment process are a key driver of abandonment.

This concern is underlined by past experience with 3DSecure: in Germany, almost 62% of merchants reported lower conversion rates in their check-out processes after the introduction of 3DSecure—and more than 35% said credit card transaction volumes declined. There were two reasons for this negative experience: first, cardholders were not accustomed to performing an additional authentication step during a credit card payment at all; and second, the authentication mechanisms used by most issuers are not very convenient.

Such experiences mean most merchants would probably like to avoid having SCA within their check-out processes whenever possible. They have two options for doing this:

USING DIRECT DEBITS: Unauthorized direct debits could be carried out without any SCA obligation, and merchants working with PISPs must manage the risks of the 13-month return period for those transactions. There is the additional risk that there is no funds-check or reservation on a direct debit payment, and there may be insufficient funds when the direct debit is processed. However, some service providers offer to manage this risk at a cost that is no higher than an average card transaction. What's more, direct debits are already the dominant payment method for e-commerce transactions in some countries: we estimate in Germany[1] 75% of all

Amazon transactions are direct debits and more than 90% of all PayPal transactions also have an underlying direct debit. This means these two large players in one of Europe's biggest e-commerce markets are already relatively immune to the new SCA requirements. It is likely that other e-commerce providers will look to follow suit by moving towards direct debits, and not only in Germany.

USING A CONSUMER 'WHITE-LIST': Consumers will be able to maintain a 'white-list' of trusted beneficiaries at their bank. For all transactions with these beneficiaries, SCA is not necessary. Typically, consumers already have a list of beneficiaries (utility companies, tradespeople, schools and so on) with account details that they have set up on their bank accounts through online and mobile banking, and we expect these will form the white-lists permitted under the RTS for SCA exemption. Additionally, we expect banks may create their own white-lists of widely-used merchants for consumers to access without setting them up separately. E-commerce merchants will work hard to get onto these lists, and banks can recommend an initial list of trusted beneficiaries to their customers. This will boost convenience for customer while also creating opportunities for banks to charge beneficiaries for inclusion on their lists.

IMPACTS ON TECHNOLOGY GIANTS SUCH AS AMAZON AND PAYPAL

Currently, e-commerce merchants are able to decide what balance to strike between strong security and a frictionless customer experience. However, the decision on whether to live with these conflicts currently lies with the merchant.

With PSD2 and RTS this situation changes completely, with merchants losing the ability to make this choice. Instead it will be up to the cardholder or account-holding payment service provider (APSP) institution to decide what the SCA will consist of. The underlying effect is that all the solutions that merchants have created to provide consumers with slick, effectively invisible payments—for example Amazon's 1-Click®, but also other models where card details are stored on file, as with Taxi Apps—will require two-factor authentication for transactions exceeding €30, unless the issuing bank deems them exempt under the RTS.

This presents a potential challenge for big e-commerce merchants such as Amazon, since it reduces their ability to strike their own desired balance between security and customer experience—and experience shows the quality of the customer experience is related directly to conversion rates. That said, merchants do have the option of avoiding the SCA requirements by making specific contractual agreements with the issuing banks, the drawback being that they will have to do this separately with every bank across Europe to cover all consumers. Among other technology giants, PayPal is in a slightly different position, since it is actually an ASPSP and can make its own choices.

IMPACTS OF THE PARTIAL PERMISSION OF SCREEN-SCRAPING

One particularly significant aspect of the EC's published RTS is confirmation of a partial repeal of the ban on 'screen-scraping' originally proposed by the EBA. In the previous version of the RTS, published by the EC in June 2017, screen-scraping was again allowed as fallback solution. In the final published version of the RTS, banks are now allowed to be exempted from the fallback solution.. As noted earlier, screen-scraping is the process by which TPPs—specifically Fintechs—access a customer's bank accounts on their behalf using the customer's own access credentials. Scenarios for this might include a customer providing their mobile banking user ID and password to a Fintech service provider so it can automatically log onto their accounts to support a frictionless service experience. However, the bank's systems think it is the customer logging on personally—and this lack of end-user visibility is at the heart of the ban of screen-scraping in previous versions of the RTS.

Under the EC's RTS, screenscraping is allowed to be used by the TPP as a fallback solution if the dedicated communication API is not available or not performing adequately—or even as alternative to the dedicated API in case the bank chooses the authenticated customer-facing interface as an alternative. But Accenture believes that the dedicated API will be the main communication channel between TPP and the banks. Many large banks plan to be exempted from offering screen scraping, and smaller banks may follow. The Fintech industry seems to be satisfied with the compromise and the resulting "soft ban" on screen scraping. This will give Fintechs time to transform from using screen scraping to using APIs.

Most banks have started implementing APIs that can be used both by internal and external consumers. In this context, internal consumers are bank-owned services including its customer front-ends, while external consumers are TPPs. By definition, the level of performance will not be different between internal and external APIs, indicating that the fallback solution would not be necessary. So banks may generally provide high performing APIs to make screen-scraping obsolete.

Most large banks already use internal APIs as a good practice to reduce complexity, improve flexibility and speed up internal innovation. These APIs can be easily exposed as external APIs as well. In these banks, customer-facing interfaces such as online banking will reuse the same APIs and the same API management platform that are used for the external PSD2 APIs. Therefore, where there are performance issues with dedicated APIs, the fallback solution with screen scraping is likely to experience the same issues. Thus, the fallback solution in these instances may not generate much benefit for TPPs and banks.

On top of this, under the RTS, banks will have to ask for two-factor authentication every time the customer logs on—a requirement that makes screen-scraping inconvenient, especially if the customer has multiple accounts with multiple banks. By extension this could also make many Fintech aggregation services unworkable, since screen-scraping is often at the heart of their business models.

Given the factors explained above relating to the fallback solution and inconvenience for data aggregators, screen-scraping can be considered a "bridge technology" that will eventually disappear.

IMPACTS OF SCA ON E-BANKING

The e-Banking functionality offered by today's banks is an important platform for users to initiate payments—and many banks already request SCA for any transaction initiated via the e-banking channel. The low-value exemption from SCA will apply for e-banking transactions as well for credit transfers using SEPA Credit Transfer payment instruments, meaning customers can initiate credit transfers on the e-banking platforms for transactions below €30 without SCA being required. As we highlighted earlier, banks will also be able to set up preapproved lists of beneficiaries not subject to SCA, derived from customers' known recurring transactions and their own accounts within the same bank. In order to increase data security, banks could also add a consent function to their online accounts, such as asking yes/no for general consent to all AISP requests.

IMPLICATIONS OF THE TRANSACTION MONITORING REQUIREMENTS

A further requirement of PSD2 and the RTS is that all ASPSPs—including banks issuing cards and offering bank accounts—will need to monitor the levels of fraud in online and mobile payments down to the level of the individual transaction. This will require a degree of monitoring far in excess of that commonly applied in the past. Combined with the need to report these fraud levels to the regulators, the result will be a significant increase in overheads and effort for banks. Generally, banks will need to implement some form of analytics capability to monitor and analyze activity and detect fraud. However, the good news for banks is that if they can keep the incidences of fraud below certain pre-defined levels for various sizes of transaction, then they will not have to apply two-factor SCA to every transaction. Additionally, with transaction analytics, banks will be able to monitor fraud much more forensically, for example by merchant or by geographic location. This will allow them to combat fraud more effectively, as well as possibly enabling them to offer services off the back of the transaction monitoring information.

These requirements may create challenge for merchants, since one type of payment card may have levels of fraud below the threshold and therefore not require SCA, while another might have fraud levels above the threshold, meaning two-factor SCA must be applied. This would make the user experience uneven for customers using different payment cards from different banks. There's a possibility that some merchants might look to avoid this requirement by agreeing to pay extra to waive the need for SCA—but banks would be unlikely to agree to this for any but the biggest online retailers. Even so, retailers would have to make arrangements with individual banks, which would inevitably concentrate on the larger banks at the expense of the smaller ones.

STANDARDIZATION

One of the greatest potential benefits of the PSD2 regime is the opportunity for greater standardization and interoperability of payments processes and technologies within individual European countries and across Europe as a whole. At a European level, progress is being made on standardization of interfaces through bodies such as the Berlin Group's NextGenPSD2, as described below. However, many initiatives currently are being driven at the national level—such as STET for France, Polish API in Poland, the CMA Open API Banking Initiative. The fact that there are so many initiatives creates a risk that API standards in Europe could become fragmented.

STANDARDIZATION IN GERMANY

For the RTS, the EBA has chosen a minimum requirement approach instead of imposing harmonization and standardization. This approach has left banks with substantial leeway in how they define the details of the new interfaces they provide to TPPs. The result could be a very fragmented landscape of open banking interfaces—and it will be a challenge for the TPPs to offer their services on a European scale if they have to implement potentially thousands of different interfaces. If this is the outcome, there will be significant room for service providers to offer API aggregation and consolidation services.

In some countries, this situation could also lead to a much more fragmented situation than has been the case up to now. In Germany, for example, the open FinTS standard promoted by the German Banking Industry Council (GBIC) has been supported by nearly all banks for almost two decades. Account information service providers like Centralway Numbers and payment initiation service providers like Sofortüberweisung have been using these interfaces for many years. Some banks have even created multibank aggregation in their online banking products on this basis.

However, GBIC has decided not to refine the FinTS standard further to make it PSD2 compliant, meaning that banks must phase out their FinTS interfaces and develop new PSD2 compliant interfaces. The German banking industry is still hoping that a pan-European standard will become available, developed by the industry to replace

FinTS. But time is running out, and a lot of German banks have already started the implementation of their PSD2 APIs. If a new industry standard is not in place in time, the adoption of PSD2 in Germany will create a payments market that is more—not less—fragmented than today's.

At the moment, the German banking industry is building on a pan-European standardization initiative set up by the Berlin Group. The Berlin Group was founded in 2004 with the primary goal of creating interoperable standards in the cards business. Over time the group's work has evolved into other interbank spheres, and its XS2A working group now has more than 40 European organizations involved in the standardization process. The Berlin Group has initiated the NextGenPSD2 working group, and published the first draft of its API standards on 2nd October 2017 for a market consultation that lasted till 17th November 2017, with the final version released by on 8th February 2018. As this is an industry-developed standard and not part of the PSD2 regulations, implementation will be voluntary. Berlin Group's NextGenPSD2 is an API framework that has an assortment of different options and allows various API standards. Currently it is not clear whether the Berlin Group will be able to come up with a widely accepted single standard, as it is competing with national standardization initiatives in various European countries, such as STET in France and PolishAPI in Poland.

STANDARDIZATION IN THE UK

The UK's Competition and Markets Authority (CMA) published its report on its investigation into the UK retail banking market in August 2016. Its package of remedies to increase innovation and improve competition in UK banking included the creation of an Open Banking Implementation Entity, now a separate company called Open Banking Ltd. This body was set up by nine leading UK banks to develop API standards that would enable different software from different financial institutions to interact and exchange data. The CMA has deliberately aligned its requirements for the Implementation Entity with PSD2—so, while not identical, they have significant areas of overlap.

The API standards that the Implementation Entity is working on will support the efficient and seamless sharing of payment and account information. The body is also developing a centralized registry so banks can check whether TPPs are registered or authorized. It is also aiming to issue policies on data redaction, liabilities and access, and on recourse in customer disputes. Since the Implementation Entity is developing a set of rules and policies that banks will need to follow to participate in the UK payments market, it does resemble a scheme in some respects. However, PSD2 mandates that there should be no contractual arrangements between the parties—so it will be interesting to see how this potential sticking point plays out.

The Implementation Entity is already well advanced in its work, having published its initial set of reference data APIs in April 2017 in areas such as ATMs, bank branches, product details and service conditions—followed by Payment Initiation and Account information in January 2018. The costs borne by the nine sponsoring banks are not disclosed, but given the size of the effort and the team in place at Open Banking Ltd, these costs must already far exceed the £20m originally estimated by the CMA. However, the nine participating banks do have the benefit of being able to help shape the standards—something which other banks, while not having to bear the costs, are less able to do (although the Implementation Entity is open to participation by all).

Overall, the UK experience has underlined the degree of industry collaboration needed to establish agreed standards. And while the Implementation Entity still has a significant amount to do in the coming months and years, the fact is that the UK is well ahead of most other jurisdictions across Europe. To operate in the PSD2 payments ecosystem, ASPSPs must be registered—or in the case of PISPs, authorized—with the competent authority in the UK, the Financial Conduct Authority (FCA). The approval processes in the UK started in October 2017, and once they're under way there'll be immediate demand for the full range of bank APIs, as well as for central registries of registrations and authorizations. With even the UK—despite being well advanced—struggling to meet the PSD2 timeline (the CMA has granted extensions to five banks), there's a real prospect of widespread fragmentation in approaches to PSD2 across Europe.

THE INTERIM PERIOD BETWEEN PSD2 AND RTS IS NOT A REASON TO DELAY IMPLEMENTATION...

It's against this background that banks are facing the interim period—or 'gap', as we termed it earlier—between the enactment of PSD2 on 13 January 2018 and the implementation of EC's RTS at a later stage. Given that the RTS will not come into force until 14th September 2019, it's clear that the gap will be substantial. However, as we highlighted earlier, banks should not take this timelag as a reason to hold back on their development of PSD2-compliant solutions. By moving now to create offering that combine a frictionless customer experience with strong security, they'll position themselves both to gain competitive edge in the market, and meet the underlying goals of PSD2 and the RTS.

...AND STANDARDIZATION REMAINS KEY

As events play out in the run-up to PSD2, it's clear that standardization is important—but also that there will inevitably be a degree of fragmentation in its implementation. Even where standards are introduced for elements such as APIs, there will be variations in the quality of the data provided by different banks—a point

illustrated by the initial wave of APIs in the UK. However, over time market forces and competition will ensure that data quality become increasingly standardized, with poorer-quality and non-standard APIs simply not being used.

Given these likely developments, banks should take steps now to anticipate the interface and process standardization being pursued by bodies such as the Berlin Group, and align their service offerings and solutions with the direction of travel to avoid playing catch-up later. Banks should also look to contribute actively to industry initiatives and regulatory consultations, with the Berlin Group once again representing a good example of these.

CALL TO ACTION

So, what do PSPs—including banks, nonbanks, merchant acquirers and online gateways—need to do to put themselves in pole position for the post-PSD2 marketplace? Some steps, such as moves to improve standardization and define the role of registries, will take place largely at an industry level. But banks and other PSPs can also make great strides individually by defining the new customer journeys and experiences under PSD2, complete with two-factor SCA.

This will essentially involve taking five steps:

1. **Identify the customer experience** they want to offer, including for online/mobile banking.
2. **Clarify the services** they want to offer online and at POS: for example, what choice will they offer merchants on SCA, and how will they price it if it is better than their online banking offerings?
3. **Develop a good customer experience** for SCA: what would that look like?
4. **Identify what solutions are available**—such as behavioral biometrics—that can both help to improve the customer experience and also meet their service offering requirements.
5. **Define how they will use exemptions** from SCA in their service offerings and customer experience.

We'll now take a closer look at the customer journey component.

NEW CUSTOMER JOURNEYS INTRODUCED BY PSD2

PSD2 helps enable two new journeys for customers which will be experienced via third party providers. These are:

- Viewing payment account(s) information via an AISP.
- Initiating payment directly from payment account via a PISP.

Each of these journeys requires a different level of customer authentication. However, the overarching message is that customers will experience SCA procedures as part of each of these new journeys. SCA is required under PSD2 in order to access payment account information online. This means applying two-factor authentication, with two out of the following three factors being taken into account:

KNOWLEDGE: something a customer knows, such as a password.

POSSESSION: something a customer has, such as a secure token.

INHERENCE: something inherent to a customer, such as a fingerprint.

Authentication methods provided by an account-holding bank can be relied on for all customer journeys. This means that a customer's experience of a new service initiated by a TPP will be influenced by their account holding bank.

INNOVATION ENABLED BY PSD2 AND STRONG CUSTOMER AUTHENTICATION

Strong customer authentication procedures for online banking is a functionally acceptable experience for today's customers. When they are logging in to view bank accounts and transfer funds, they expect and prepare for security procedures to be applied to protect them. So customers are well-accustomed to authenticating themselves in order to access these fundamental services, and accept the need to do this. Going forward, where a PISP relies on the account holding bank for authentication, it is likely that there will be a disconnect in customer's expectations of new services enabled by third parties under PSD2. The traditionally acceptable methods of authentication may not be consistent with the new innovative journeys that are enabled by APIs, but customers will need to accept them in order to access those PISPs' services.

As these new solutions gain traction, it is likely that we will see partnerships being formed between new TPPs and account-holding banks to help broaden the financial and non-financial ecosystem of both parties. In these cases, we can expect to see innovative solutions introduced to the authentication process, which will tie in with the new products on offer. For example, new TPPs are not limited to mobile/

tablet and desktop to provide services. We should expect these services to take full advantage of the API ecosystem, internet of things (IoT) and artificial intelligence (AI), with customers' experiences expanding rapidly to include non-banking APIs and wearable technology. We can also expect to see biometrics and biometric profiling playing a much larger role in SCA processes.

As these developments gain pace and momentum, the customer experience will differ depending on which bank a customer selects for account access, and the partnerships that PISPs—and to a lesser degree AISPs—will form. Overall, the balance between security and innovation is critical in the customer experience of new services enabled by PSD2, and the providers that strike the best balance will be well placed to win in the marketplace.

WILL THERE BE FURTHER INNOVATION IN STRONG CUSTOMER AUTHENTICATION?

The following use cases will require quick and seamless SCA to help enable the customer to buy at pace—raising the question of whether the account holding bank will partner with the relevant TPP to create a seamless IoT/AI compatible two-factor SCA process.

SAMPLE USE CASE 1: Social media company disrupting traditional shopping customer journey by acting as an AISP/PISP

- Social media companies acting as AISPs can provide more targeted advertising focused on what customers would like to buy, based on historical spending data.
- As PISPs, social media companies can provide a one-click sales process on adverts. And by charging origination fees to the retailer, they can also tap into a new revenue stream.
- A social media company can even become both an AISP and PISP, enabling it to provide more targeted advertising and seamless checkout options, as well as enhancing the customer experience and generating new revenues.

SAMPLE USE CASE 2: Smartphone manufacturer providing a 'request to pay' service

- The UK is introducing a 'request to pay' direct debit instruction. For example, a customer will be notified that they 'owe Rory £10' and invited to pay him that amount.
- A smartphone provider as a PISP could send the customer a 'request to pay' notification, and the customer could pay via Siri, reducing the cost of collections and the number of inaccurate payments.

CONCLUSION

Now that the PSD2 is in force, and the RTS for SCA are final we believe the message is clear. Now is the time to embrace the opportunities that PSD2 presents. The place to start is by devising the right customer experience—and understanding how this can be balanced with the more stringent authentication required under PSD2.

Whatever the precise timescale, the PSD2 world is coming—and banks will need to be ready for it, or face a struggle to catch up with faster-moving competitors.

The goal for customers is frictionless services that provide a compelling, differentiated experience and keep their data and money secure. Any bank that moves today to provide such services will be well placed both to outpace the competition—and also to comply with PSD2.

CONTACT US

Hakan Eroglu
Financial Services, Accenture Switzerland
hakan.eroglu@accenture.com

Andrew McFarlane
Financial Services, Accenture Ireland
andrew.g.mcfarlane@accenture.com

Oliver Hommel
Financial Services, Accenture Germany
oliver.hommel@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com

ABOUT ACCENTURE PAYMENT SERVICES

Accenture Payments, a business service within Accenture's Financial Services operating group, helps banks improve business strategy, technology and operational efficiency in three key areas: core payments, card payments and digital payments. Accenture Payment Services and its more than 4,800 professionals are dedicated to helping banks simplify and integrate their payments systems and operations to reduce costs and improve productivity, meet new regulatory requirements, enable new mobile and digital offerings, and maintain payments as a revenue generator. More than 50 clients worldwide have engaged Accenture Payment Services to help them turn their payment operations into high-performing businesses. To learn more, visit www.accenture.com/us-en/banking- payments-services.