EXECUTIVE BRIEF | AUGUST 2015

ca technologies

CA Viewpoint

Global Regulatory Trends for Mobile Payments and How CA Can Help

International Regulatory Trends for Securing Mobile Payments

The aim of this document is to provide:

- An overview of key regulatory trends impacting the mobile payments ecosystem
- A snapshot of the factors to be considered for mobile payment authentication
- Insights into how banks can cost effectively implement payment authentication solutions that address regulatory mandates and guidelines for secure mobile payment transactions

Mobile payments (M-payments) are growing rapidly around the world allowing consumers to pay for goods and services at any time and in any location. In 2014 the number of mobile devices was reported to be over 7.2 billion[1], officially surpassing the number of human beings on the planet and reached over 7.5 billion as of the writing of this briefing document. Growth in the number of mobile devices is multiplying five times faster than people—population growth rate estimates are 1.2 percent[2] annually, or about two people per second. This phenomenal increase can be attributed to mobile device use for managing day-to-day personal and business activities, and the popularity of social media.

High mobile device penetration—particularly across the developing world—along with advancements in technology, changes in consumer preferences and increasing competition in the payments value chain are key drivers in development of new banking platforms and new mobile payment solutions. Along with the growth in mobile technology, it is not unexpected to see increasingly sophisticated criminal activity. A supportive regulatory framework, a secure infrastructure, implementation efficiency and innovation in electronic payments are crucial if consumers, banks, retailers and other m-payments stakeholders are to experience continued socio-economic benefits.

Regulators and banks around the globe are responding and adapting to the accelerated advancements rising from the mobile payments industry. Countries are enacting regulatory frameworks for mobile payments that are heavily focused on consumer protection and with an eye towards ensuring competition in each unique market space. Another aspect of policy goals is to encourage interoperability among the various mobile payments stakeholders to lower cost and support the widespread adoption of mobile payments. Sector-specific standards, government policies and consumer-protection frameworks need to be aligned, and practical implementation strategies for financial institutions are critical since banks typically shoulder the heaviest responsibility for ensuring that services within a mobile payment ecosystem meet the entirety of regulatory requirements.

The full picture is complex, requiring industry-wide partnerships as regulators, banks and solution providers have increased focus on security, convenience and speed of payments. As such, this document is intended discuss about regulatory trends for m-payments and provide insight into how CA Technologies payment security solutions can help address such mandates. The overarching themes have been identified with the goal of providing an understanding of regulatory implications for mobile payment authentication.

Global Regulatory Trends Impacting the Mobile Payments Landscape

Making Internet payments convenient and secure for customers and mitigating the risks associated with processing card-not-present (CNP) payment transactions is of paramount importance so that the payments ecosystem progresses to the benefit of individuals, companies and governments alike. International policy and legislative developments relating to cyber-security, data security, identity security, ecommerce transactions and Internet payments have been receiving unprecedented attention.

The engagement of many stakeholders is important with banks in particular shouldering the heaviest burden in making sure implementations meet standards and legislative requirements, facilitate secure transaction processing and map business practices to appropriate risk levels. Also, new non-bank entrants into the payments ecosystem are growing, so managing new risks that arise from these entities requires strong payment industry leadership. To address specific concerns around mobile payments, the approach by regulators centers around two areas: forming industry working groups to identify best practices and reach agreement on guidelines for compliance and drafting legislation, regulations and new directives for stakeholder compliance

While market dynamics differ in each country, key regulatory themes across jurisdictions are centered on protecting consumers, mitigating fraud, increasing consumer trust and striking a balance between industry cooperation and competition.

Central policy issues:

- Cyber security
- Data security
- Identity security
- Security breach notification systems
- Ecommerce
- Internet banking
- Card-not-present payments
- User authentication

Regulatory framework

Legislative frameworks help achieve widely applied industry and international standards and typically cover the following three aspects:

- Operational processes: to enhance the user experience through standardized processes
- Security requirements: to ensure the security of cardholder data and online payment services
- Technical standards: to facilitate interoperability across different infrastructures, mobile devices, software interfaces and point-of-sale terminals

As we consider Internet and mobile payments, inclusion of all the stakeholders is critical to achieve the highest global standards; make the ecosystem convenient and secure for customers; and mitigate risk for banks, merchants and payment service providers. Unified solutions must include infrastructure providers, software developers,

Key regulatory themes from around the world are summarized as follows:

- Protect Internet payments and access to sensitive payment data using strong customer authentication
- Operate transaction-monitoring tools to prevent, detect and block fraudulent payments and subject high-risk transactions to specific screening and evaluation before the transaction is completed
- Security breach notification systems and sharing cyber-security-threat information with key industry stakeholders and governments
- Set limits for Internet payment services and provide customers with options to further limit risk including alerting and profile management services
- Ensure that customer enrollment and authentication provisioning is carried out in a secure manner
- Incorporate multiple layers of security defenses
- Have processes in place that ensure all transactions are properly traced
- Limit the number of login or authentication attempts, session length and one-time-password (OTP) time of validity
- Protect sensitive payment data when stored, processed or transmitted

makers of hardware, chip developers, mobile network operators and personal computer and handset manufacturers. Standards organizations and cross-industry consortia, such as EMVCo, International Organization for Standardization (ISO) and the Near Field Communication (NFC) Forum have long maintained an eye on trends impacting the CNP payments landscape and have focused expertise on the mobile payments ecosystem with well-established collaborative efforts for creating secure interoperability standards.

Working groups made up of these key stakeholders serve an important function in sharing market research, best practices, ideas on achieving interoperability and reaching consensus on approaches for implementation. These groups work to develop principles that support mobile industry efforts to voluntarily self-supervise, assisted by regulatory agencies. Support and participation in these working groups from industry is particularly important for staying ahead of criminal elements, since legislative directives need to evolve in order to sufficiently address changing market dynamics for ecommerce and mobile payments. Examples of regulatory working groups include:

- The U.S. Federal Reserve convened the Mobile Payments Industry Workgroup
- The European Central Bank supervises the European Payments Council
- The Korean Communications Commission formed the Grand NFC Korea Alliance

Every region expects significant growth in m-payments. The mandatory provisions enacted by policymakers around the world correlate to the type of growth seen in each market for ecommerce, Internet payments and mobile banking. High-level policy issues tend to focus on cyber security, data security, identity security, security breach notification systems, ecommerce, Internet banking, remote payments and user authentication. Some regulations within each region related to these issues are outlined in the attached Appendix A, and we have provided a list of links below for anyone wishing to further explore regulations around the world.

Market trends

Adoption of mobile devices for electronic payments, mobile banking and electronic financial services varies from country to country. In particular, the type of service evolving is driven by consumer lifestyles and socio-economic development. Countries with emerging economies, such as many in Asia-Pacific, Africa and Latin America are dominated by trends in adopting mobile money solutions for unbanked and under-banked consumers. North America and the European Union (EU) tend to drive most of the new payment technology advancements and exhibit high growth potential for mobile payment solutions. The Asia-Pacific region is expected to overtake North America to be the largest online retail market within a few years—driven heavily by China, South Korea and Japan—so the growth of online payments in these countries has been of particular interest to the industry and regulators.

The U.S. and Canada share high consumer satisfaction with credit and debit card usage. There is significant growth in electronic payment forms and use of mobile devices for banking and payments. U.S. regulators want to avoid potentially stifling innovation by creating new rules while industry is developing mobile technology and creating businesses. The approach as been to adapt the current consumer protection rules relevant to m-payments in anticipation of new challenges and issues as the technology evolves.

Canadian consumers are increasingly moving away from branch-based banking towards online and mobile banking so the scope of m-payment regulation is towards extending current consumer protection to the mobile landscape and solving new issues related to fraud and privacy.

Europe has strong market readiness, movement towards various forms of electronic payments, and high mobile phone penetration and mobile banking adoption. Regulatory directives in Europe are typically principles-based, technology neutral and strive for adaptability. But consumer-protection rules are vital across all EU countries while allowing individuals to divulge personal data when it is in their own interest. These policies are driven to ensure that the harvesting and processing of customer data is lawful and fair. You can refer to CA Viewpoint on the European Banking Authority (EBA) guidelines[3] for more detail on how CA can help address EU payment service directives.

Online shopping remains the leading purpose for credit card use in Australia driving the need to ensure user authentication techniques protect customer data and banks have effective risk management.

In many markets where online and mobile payments are dominated by local third-party payment providers and mobile network operators, government regulations attempt to further the growth of online payments through entrepreneurial innovations and protect consumer rights with mandates for multi-factor authentication and single message systems (SMS) for user authentication. This can be seen in China, South Korea and Japan where rates of consumer adoption and m-payment transaction volume are the highest worldwide.

In developing markets where most of the population lives in remote areas, people are more likely to have access to mobile phone networks than basic financial services. For instance, mobile device penetration is over 75 percent in Kenya where only 4.23 percent of adults have a bank account. Approximately 83 percent of all mobile subscriptions worldwide are in the developing world, but the proportion of individuals over the age of 15 that have a debit card is 34.5 percent in the East Asia and Pacific region, 9.1 percent in the Middle East and 7.2 percent in North Africa3. This market situation has led to the emergence of successful models for mobile banking with programs such as Safaricom's M-Pesa in Kenya. The continued proliferation of mobile money offerings is helping to fill the gaps in financial services availability and has provided impetus for extensive consumer-protection regulatory initiatives.

In addition to the information above and reference Appendix sections, we have provided a list of links below for anyone wishing to further explore market trends and some specific regulations around the world.

The diversity of market drivers and the enormous complexity of complying with regulations, along with consumer choice in mobile payment have amplified both the cost and effort required by financial services companies to implement m-payment solutions. Heavy fines can result to banks from failing to comply, affecting the financial bottom line and reputation in the marketplace. The payment security solutions from CA Technologies go a long way to help banks address the necessary compliance with regulatory mandates and build a robust risk management toolbox, with state-of-the-art mobile authentication solutions.

Mobile Authentication

Mobile devices have taken the world by storm with our devices becoming a part of who we are as individuals. Mobile devices have enhanced consumer choice and ability to access product and services. With this convenience also comes risk, and banks must adopt strategies in line with changing consumer behavior and mobile technology advancements to remain competitive and gain market share in the banking and payments arena.

As mentioned above, regulatory frameworks strive towards protecting the privacy and data of consumers. Ecommerce transactions typically generate a trail of behavioral data, browsing habits and purchasing characteristics. Mobile devices easily store data about purchases, geographic location, travel patterns and personal details. Regulators are trying to balance the need to encourage the growth of mobile technology with the obligation to protect consumers from new issues that are bound to arise. Regulatory mandates for protecting consumers from payment fraud include recommendations for implementing advanced authentication technology and enabling strong authentication for high-risk CNP transactions. Authentication solutions for mobile payments should also be designed to protect the confidentiality of the authentication data.

Mobile devices are now used for everything, with the evolution being tied to a user's identity and as well as a payment device. The rapid increase in mobile device use for performing Internet banking and online payment transactions increase the fraud incurred by banks, merchants and legitimate customers, making it even more difficult to remain competitive in the payment industry. In order to be successful, banks must deploy intelligent solutions that strike the right balance of security and customer experience, all while making sure operational costs are kept to a minimum.

Authentication is all about finding out whether a user really is who they claim to be. Industry leaders have actively worked to stay ahead of criminal elements in securing cardholder data and authenticating legitimate payment activity for many years, with technology such as 3D Secure, one of the earliest established payment authentication

schemes. Deploying a highly secure solution that stops fraudulent transactions, improves operational efficiency and creates a smooth experience for legitimate customers is the only way for banks and merchants to remain ahead of the competition.

A first line of defense in reducing CNP fraud is the use of advanced models to identify legitimate transactions. The ubiquity of mobile devices and the inherent proprietary nature to an individual user's behavior supports real-time risk analytics as a fundamental element for increased strong authentication through validating a legitimate user while providing a secure, frictionless checkout experience.

Mobile devices naturally lend themselves to becoming tools for strong customer authentication that includes a multi-factor authentication interface, with a layer of security that is unique to customers and helps organizations simplify legitimate user authentication and reduce fraudulent activity.

By focusing risk practices on data management, banks can comply with key regulatory mandates, increase operational efficiency and launch new services. This approach will help banks to recoup some of the investment they have made in complying with an increasing number of ever more complex regulations. CA Technologies understands what is necessary to stay ahead of rising fraud, with new authentication techniques as well as new mobile capabilities for contactless payments that will make this a reality.

How CA Technologies Payment Security Products Help

Having a solid authentication strategy is the foundation in addressing many of the legislative mandates related to Internet and mobile payments, regardless of the type of device a banking customer uses for payment transactions. As a leading provider of Internet payment security solutions, CA Technologies is the ideal partner to support banks to cost effectively implement a powerful CNP payments foundation, create a seamless customer experience and help banks address regulatory standards and policy mandates set forth by government legislators and standards organizations.

The line-up of payment security solutions from CA Technologies:

- **CA Transaction Manager** supports implementation of 3D Secure (3DS) so that each transaction can be authenticated. This product solution is used by over 13,500 bank portfolios with over 165 million active cardholders worldwide.[4] More issuers are choosing CA Transaction Manager everyday because it enables a dynamic and personalized online shopping experience. And, because our payment security product team has been involved with developing 3DS[5] technology since initial establishment of the secure protocol, CA Technologies can provide seamless 3DS compliance with Verified by VISA®, MasterCard® SecureCode, JCB J/Secure™, American Express SafeKey® and Discover/Diners ProtectBuySM cardholder authentication programs.

- **CA Risk Analytics** uses sophisticated neural network modeling to identify and isolate CNP fraud with zero-touch 3DS authentication. This CA product solution allows banks to dynamically customize rule settings according to individual financial institution fraud and risk policies giving comprehensive control over fraud thresholds and implementing individual bank business policies. Advanced behavioral predictive models and dynamic rules are used to assess the potential risk of each transaction and instantaneously deny, alert, allow or require additional authentication for each transaction as appropriate. No explicit cardholder interruption occurs during the checkout process unless additional verification is triggered based on the scoring results.
- **CA Strong Authentication** provides simple, intuitive and dynamic authentication that aims to address most legislative definitions of strong customer authentication. This product solution provides multiple options for multi-factor authentication including OTP via SMS, voice or email, and a Mobile OTP app providing instant OTP generation, two-way notifications and secure passwords for both Internet payments and access to sensitive payment data. Offered on-premise or as a cloud service, CA Strong Authentication delivers user friendly alert capability for the cardholder to confirm valid transactions. Using two-way notification solutions, a transaction identified as potentially fraudulent can be validated instantaneously by cardholders from their mobile device, allowing them to complete their transaction or identify the transaction as fraudulent. This versatile authentication solution from CA Technologies enables multiple authentication modes including a two-factor soft credential, OTP delivered via SMS or voice, Mobile OTP application, two-way notification and other multi-factor options.

Additional CA Technologies product solutions can further protect banking customer experiences and help mitigate threats and comply with regulations. For instance, CA Privileged Identify Manager provides fine-grained privileged user access controls, shared account password management, authentication bridging and user activity reporting—in both physical and virtual environments for privileged banking users. CA Single Sign-On (SSO) provides for a unified login experience for access to online banking applications.

The rapidly evolving regulatory landscape, increasing sophistication of fraudsters and the desire for an improved customer experience has already led a significant number of banks worldwide to choose our mobile authentication solutions. Existing CA Technologies customers can quickly enhance their payment authentication products by working with us. We have created Appendix B for easy reference to our solutions. You can review how CA payment security solutions are designed to address key regulatory categories in Appendix C of this document and you can work with our account specialists to explore what authentication solutions will best suit your business needs.

What's Next?

Contact us today. We can advise you on what payment security products from CA Technologies may suit your needs and work with you to implement the best secure authentication options as your bank works towards compliance with regulatory mandates and guidelines.

We are committed to work closely with CA customers and partners to fully deliver solutions designed to increase customer loyalty, grow revenue and address compliance with the higher security standards required under current and future regulations.

Learn more about CA Technologies payment security products at www.ca.com/payment-security or send an email to paymentsecurity@ca.com to connect with a product expert. CA Technologies customers can contact their account representative for a detailed assessment on how our payment security solutions can support your bank's mobile payment products.

Appendix A

Overview of Global Legislation Related to Internet Payment Security

The policies referenced in this document are not exhaustive. Overarching regulatory themes have been identified to address business considerations for mobile payment authentication. We have provided links to some of the referenced regulatory bodies for anyone wishing to further explore this topic.

Internet Payments and Mobile Payments

	eCommerce	Mobile Commerce	Authentication		
			Multi-Factor Authentication (MFA)	One-time Passwords (OTP)	Single Message Services (SMS)
Global Oveview	**Asia Pacific:** South Korea's Electronic Financial Transactions Act (2007) outlines detailed rules concerning the responsibilities of banks and nonbanks to provide redress to consumers. The South Korean Consumer Protection Act (ECPA) enacted in 2002 and revised effective 2006 requires consumers be given detailed information about their purchases and allows them to either confirm purchases or make changes before authorization; information disclosed by the consumer during the transaction must be protected by both the merchant and the payment service provider. **Europe:** European Central Bank (ECB) led efforts with the European Banking Authority (EBA) and the European Forum on the Security of Retail Payments (SecuRe Pay). 2013 recommendations to increase retail payment security and security of electronic payment services and instruments to ensure consistent Internet payments. Guidelines are based on the regulations set out in the EU Payment Security Directive (PSD) and PSD2. **Middle East:** Saudi Arabia issued e-Commerce protection laws in 2007.	**Africa:** Kenya extended regulations under the payment system rules beyond banking to MNOs, like M-Pesa, especially related to money transfer activities. Nigerian Central Bank regulatory requirements for mobile payment solutions and services forbids allowing the use of prepaid airtime value for payments or money transfers. **North America:** The Canadian Department of Finance 2010 enactment of mobile payments in Code of Conduct for the Canadian Credit and Debit Card Industry. **South America:** In 2013 and 2014 Brazil adopted regulations for online and mobile payments that created the possibility for the normalization of mobile payment systems and the creation of electronic currencies.	**Asia Pacific:** In 2005 the Hong Kong Monetary Authority (HKMA) required banks in Hong Kong to implement two-factor authentication (2FA) for high-risk services to comply with the Personal Data Privacy Ordinance (PDPO) and any relevant codes of practice, rules or guidance issued or approved by the Office of the Privacy Commissioner for Personal Data for protecting personal data of their customers. One major type of 2FA method adopted by banks is to generate a one-time password (OTP) and send it to their customers' mobile phones through SMS message. **Europe:** European Banking Authority (EBA) recommendation for implementing multiple layers of payment security defense with strong authentication. **India:** The Reserve Bank of India 2014 Operative Guidelines for Banks requiring double factor authentication to secure card-not-present (CNP) transactions. **North America:** In the United States, President Obama issued a 2014 Executive Order mandating multi-factor authentication intended to improve security of online financial transactions. Updates guidance is still under development. The 2012 US Federal guidelines recommend multiple layers of security controls beyond the traditional username and password, particularly for out-of-band authentication methods.	**Asia Pacific:** 2005 bank requirement from the Hong Kong Monetary Authority (HKMA) for implementing two-factor authentication (2FA) for high-risk services with the major type of 2FA being a one-time-password (OTP). **Europe:** European Banking Authority (EBA) recommendations when using a one-time password (OTP) for authentication purposes, payment service providers should ensure that the validity period of such passwords is limited to the strict minimum time necessary.	**Africa:** Egypt has mandated increased non-SMS authentication security requirements. **Asia Pacific:** HKMA implementation of stringent restrictions against forwarding a OTP SMS. The controls for SMS forwarding were agreed with the telephone operators to deliver SMS OTP messages originating from banks (and EPS Company (Hong Kong) Limited, EPSCO), to the registered mobile phone of the customers regardless of whether the SMS forwarding service of that particular mobile phone number has been activated. **Europe:** Although specifically excluded from the scope of the EBA guidelines (payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology), European country specific implementations and restrictions vary. One example includes the German Central Bank (Bundesbank) mandate that OTP via SMS can be considered to be a 2FA as long as the purchase and payment process are not done from the device that gets the SMS, thus requiring two separate devices for a cardholder to support mobile online payments.

Cyber-security

Europe: Legislation on Network and Information Security (NIS) is being discussed at European level. The Directive aims to facilitate information sharing between member states and private and public sector organizations on cyber-security threats. Organizations across the EU will need to address complex technical, governance, and process challenges. It will also introduce a security breach notification system and baseline security requirements.

Germany: An IT security law was approved earlier this year, mirroring objectives of the European NIS legislation and focused on critical infrastructure operators. It also introduces mandatory reporting requirements and security requirements.

United States: President Obama issued a 2015 advisory Executive Order urging companies to share cyber-security-threat information with one another and the Federal government. Cyber threat information sharing is pending before both the House and Senate.

Data Security and Consumer Protection

Asia Pacific: South Korea is striving to balance the promotion of mobile banking with protecting consumers from the risks that arise from m-payments in the Electronic Financial Transaction Act (EFTA) and the E-commerce Consumer Protection Act (ECPA).

Identity Security

Europe: European Parliament approved adoption in 2014 of the electronic identification and trust services (eIDAS) for e-Identification, e-Authentication and e-Signature Regulation for mutual recognition of electronic identification; sets rules for trust services, in particular for electronic transactions; The regulations as proposed by the Council of the European Union creates a legal framework for electronic signatures based on Public Key Infrastructure (PKI) and smart cards. The wireless PKI mobile digital signature solutions are currently being used in several EU countries. The regulation helps define secondary legislation on how this will be implemented in different European Member States including what authentication schemes are approved by national regulators in each EU country for cross-border purposes.

Appendix B

CA Technologies Payment Security Solutions

We are committed to work closely with CA customers and partners to fully deliver authentication solutions that increase customer loyalty, grow revenue and address compliance with the higher security standards required under current and future regulations. We are also confident that new and current users of our ecommerce solutions will be well positioned to address regulatory guidelines mandated for payment transaction authentication, strong authentication and multi-factor authentication.

Customers can quickly enhance their products by working with us, but the following outlines some initial considerations.

Considerations for current CA Technologies payment security customers

If you are using:	Then upgrade to:	Rationale:
CA Transaction Manager	CA Strong Authentication	CA Transaction Manager customers who currently use static passwords alone for 3DS authentication should consider deployment of CA Strong Authentication to help meet the requirements that include a two-factor soft credential; OTP via SMS, voice, email; Mobile OTP generator and two-way notification and transaction verification.
CA Transaction Manager and CA Strong Authentication	CA Risk Analytics	By using CA Strong Authentication, you can address most policy requirements for strong customer authentication. However, we recommend adding CA Risk Analytics to improve the customer experience. This provides a frictionless checkout experience for genuine cardholders and only suspicious transactions will require additional authentication. CA Risk Analytics can also help you increase security and reduce fraud for ecommerce transactions.
CA Transaction Manager and CA Risk Analytics	CA Strong Authentication	CA Risk Analytics can identify and block suspicious transactions. However, you will still need CA Strong Authentication to address regulatory guidelines requiring strong customer authentication to verify the genuine cardholder.

Appendix C

Below are some considerations for major regulations seen around the world and corresponding CA Technologies product solutions addressing the related issues.

Considerations for meeting key regulatory mandates for payment authentication

Regulatory Issue	Solution	Application of CA Technologies Payment Security Solution
Protect Internet payments and access to sensitive payment data using strong customer authentication[3]	CA Transaction Manager CA Strong Authentication CA Privileged Identity Manager	CA Transaction Manager implements 3D Secure (3DS) so that each transaction can be authenticated. CA Strong Authentication provides multiple options for multi-factor authentication including OTP via SMS, Mobile OTP app, two-way notifications and unbreachable passwords for both Internet payments and access to sensitive payment data. CA Privileged Identity Manager provides t fine-grained user access controls, shared account password management, authentication bridging and user activity reporting—in both physical and virtual environments for privileged user.
Operate transaction monitoring tools to prevent, detect and block fraudulent payments and subject high-risk transactions to specific screening and evaluation before the transaction is completed	CA Risk Analytics	CA Risk Analytics provides real-time analysis of each transaction, applies advanced 3DS authentication models, and produces a score that identifies both legitimate and high-risk transactions. Dynamic rules allow you to apply customized business policies.
Security breach notification systems and sharing cyber-security-threat information with key industry stakeholders and governments	CA Risk Analytics	CA Risk Analytics has capability in data aggregation within consortia participants, real-time neural network learning and continuous optimization, and analysis can be implemented so that changing fraud dynamics are calculated and identified within minutes of an emerging fraud trend. This allows for optimal escalation response when necessary.
Set limits for Internet payment services and provide customers with options to further limit risk including alerting and profile management services	CA Transaction Manager CA Risk Analytics CA Strong Authentication	CA Risk Analytics can analyze a transaction and determine the level of risk. An alert can be sent to customers, step-up authentication triggered or the transaction denied based on bank policies. CA Strong Authentication can send an OTP via SMS, email or voice, or initiate two-way customer notification so that the customer can respond immediately to continue a transaction.
Ensure that customer enrollment and authentication provisioning is carried out in a secure manner	CA Strong Authentication	Provides secure enrollment, FYP and de-provisioning workflow that use multiple forms of authentication and account activation to verify the user during creation of the account. When implemented with the CA Mobile OTP for Payments solution, provides options for multi-factor authentication including OTP via SMS, Mobile OTP app, two-way notifications and unbreachable passwords.
Incorporate multiple layers of security defenses	CA Transaction Manager CA Risk Analytics CA Strong Authentication	The combination of these products will allow you to adress the requirements for strong authentication and transaction monitoring achieving “defense in depth” for Internet payment transactions.
Have processes in place that ensure all transactions are properly traced	CA Transaction Manager CA Risk Analytics	CA Transaction Manager implements 3DS so that each transaction can be authenticated. CA Risk Analytics provides additional authentication data and an audit trail for each transaction. Case Management capabilities provide “true” fraud data.
Limit the number of login or authentication attempts, session length and OTP time of validity	CA Strong Authentication CA Single Sign-On	With CA Strong Authentication, issuers can choose limits for authentication attempts. CA Single Sign-On can incorporate logins from multiple channels.
Protect sensitive payment data when stored, processed or transmitted	Internal bank policy, however CA products do this for the data we manage	CA Technologies maintains secure, Payment Card Industry (PCI) compliant, SSAE 16 audited eCommerce Solution data centers so that data transmitted during the authentication process keeps cardholder data protected.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

1 GSMA Intelligence real-time tracker. See: https://gsmaintelligence.com.

2 United States Census Bureau world population international database. See: http://www.census.gov/popclock/.

3 Source: World Bank, 2012

4 Source: CA Technologies data first quarter of calendar year 2015

5 CA Technologies payment security solutions provide seamless 3D Secure compliance with Verified by VISA®, MasterCard® SecureCode, JCB J/Secure™, American Express SafeKey® and Discover/Diners ProtectBuySM cardholder authentication programs. For more information about 3D Secure™ technology visit www.ca.com/payment-security.

Additional References:

- European Banking Authority, guidelines on Internet payments security. See http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments
- European Parliament, Council for the European Union. See: http://certifiedsignature.eu
- See http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions
- United States President Advisory Executive Order. See: http://www.federaltimes.com/story/government/cybersecurity/2015/02/13/information-sharing-executive-order/23353405/
- Mobile payments in Brazil. See: http://www.researchandmarkets.com/reports/2694197/hot_topicmobile_payment_services_in_brazil#relb1
- Reserve Bank of India, Operative Guidelines for Mobile Payments in India See: http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365
- Mobile Usage at the Base of the Pyramid in Kenya. http://www.infodev.org/articles/mobile-usage-base-pyramid-kenya

CS200-146508_0815