Mobile and Contactless Payments Glossary

Version 1.0

Date: September 2017

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

About the Mobile and Contactless Payments Working Committee

The goal of the Mobile and Contactless Payments Working Committee is for all interested parties to work collaboratively to explore the opportunities and challenges associated with implementation of mobile and contactless payments in the U.S. market, identify possible solutions to challenges, and facilitate the sharing of best practices with all industry stakeholders

EMV is a trademark owned by EMVCo LLC.

Table of Contents

1. Introduction and Objectives

This document is a collection of mobile and contactless payments terms and definitions collected from existing U.S. Payments Forum and Secure Technology Alliance mobile/contactless payments glossaries as well as previously undefined terms provided by ecosystem stakeholders. The intent is to garner cross-industry understanding of mobile and contactless payments terms and encourage the standardization of terminology.

The Mobile and Contactless Payments Working Committee uses a broad definition of "mobile and contactless payments" to mean all non-contact payment approaches that facilitate convenient, fast and secure payment transactions for consumers. Activities will include all mobile payments approaches (e.g., bar code, QR code, Near Field Communication (NFC), Samsung Magnetic Secure Transmission (MST), EMV and Magnetic Stripe Data (MSD) contactless, Bluetooth, in-app, m-commerce browser transactions, other mobile technologies that can be used to enable payment), all form factors (e.g., dual-interface EMV chip cards, mobile devices, wearables and cards on file), and both card and non-card (e.g., faster payments) approaches.

The project scope is bounded to mobile payments with POS interactions. (In-app or mobile-based browser payment are in scope if they are used at the POS.) E-Commerce transactions are out of scope for this document.

2. Target Audience

- Moderately technical audience
- All U.S. Payments Forum members interested in mobile and contactless payments

3. Terms and Definitions

To facilitate a common understanding of terms, the project has listed key terms and definitions specific to mobile payments with POS interactions, including loyalty/reward cards. References are included for the source of the definitions, with sources below.

1. Referenced from the Secure Technology Alliance Glossary: Mobile and Contactless Payment Terms, January 16, 2017
2. Referenced from the U.S. Payments Forum Communications & Education Working Committee Standardization of Terminology document v2.1, January 2014
3. Referenced from Conexxus Mobile Payments Standard v2.0 documentation, September 18, 2016
4. Referenced from www.iso.org
5. Referenced from www.emvco.com
6. Referenced from the Secure Technology Alliance white paper: Smart Cards and Biometrics, https://www.securetechalliance.org/publications-smart-cards-and-biometrics/
7. Referenced from Wikipedia and the Secure Technology white paper: BLE 101, http://www.securetechalliance.org/publications-bluetooth-low-energy-ble-101-a-technology-primer-with-example-use-cases/
8. Referenced from https://developer.visa.com/products/visa_direct/guides
9. Referenced From U.S. Payments Forum white paper: Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud, http://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud-webinar/

10. Adapted from the Secure Technology Alliance white paper: Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization, http://www.securetechalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/
11. Adapted from the Secure Technology Alliance white paper: Transit and Contactless Open Payments: An Emerging Approach for Fare Collection, https://www.securetechalliance.org/publications-transit-financial-2011/
12. Referenced from the Federal Reserve Faster Payments Task Force and Secure Payments Task Force glossary of terms https://fedpaymentsimprovement.org/resources/glossary/
13. Referenced from PC Magazine glossary: http://www.pcmag.com/encyclopedia/term/66741/geofence
14. Referenced from PC Magazine glossary: http://www.pcmag.com/encyclopedia/term/63271/geolocation
15. Adapted from Consult Hyperion WP: http://www.chyp.com/wp-content/uploads/2015/01/HCE-and-SIM-Secure-Element.pdf
16. Adapted from http://www.itbusiness.ca/news/digital-wallet-showdown-masterpass-vs-v-me/34179
17. Adapted from https://www.nfcworld.com/2013/03/20/323195/mastercard-fights-back-against-new-payments-players-with-increased-transaction-fees-for-digital-wallets-that-dont-share-data/
18. Adapted from various Secure Technology Alliance white papers
19. Adapted from Wikipedia
20. No definitive source
21. Referenced from the Secure Technology Alliance white paper: The Changing US Payments Landscape
22. Referenced from Secure Technology Alliance white paper: Mobile ID Authentication, http://www.securetechalliance.org/publications-mobile-identity-authentication/
23. Referenced the Federal Reserve Bank of Boston white paper: Getting Ahead of the Curve: Assessing Card-No-Present Fraud in the Mobile Payments Environment. https://www.frbatlanta.org/-/media/documents/rprf/rprf_pubs/2016/11-getting-ahead-of-the-curve-assessing-card-not-present-fraud-2016-11-18.pdf
24. Referenced from Dictionary.com: http://www.dictionary.com/browse/wearable
25. Referenced from https://www.iso.org/standard/56692.html

Term	Also Known As (AKA)	Industry Stakeholder Definition
3-D Secure / 3-D Secure 2.0 (3DS)		Three-Domain Secure (3DS) is a messaging protocol to enable consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases.[5] For information on 3DS and 3DS 2.0, please see the Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud white paper.[9]
Bar Code		An optical machine-readable representation of data about the object to which the bar code is attached. Originally, bar codes represented data by varying the widths and spaces between parallel lines, referred to as linear or one-dimensional (1D) bar codes. They evolved to use rectangles, dots, hexagons, and other geometric patterns in two dimensions (2D). Mobile payments can use QR codes or other 2D bar codes.[1]

Term	Also Known As (AKA)	Industry Stakeholder Definition
Biometric Recognition		Automated methods of identifying or verifying the identity of a person based on unique biological (anatomical or physiological) or behavioral characteristics.[6]
Bluetooth		Bluetooth is a wireless technology standard for exchanging data over short distances (10-100m, using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices. Bluetooth is managed by the Bluetooth Special Interest Group http://www.bluetooth.com.[7]
Bluetooth Low Energy (BLE)		Bluetooth low energy (BLE) is a wireless computer network technology designed and marketed as Bluetooth Smart by the not-for-profit non-stock corporation Bluetooth Special Interest Group (SIG). BLE is a subset of the Bluetooth 4.0 specification. BLE was designed to require less power and incur lower cost than Bluetooth, while providing a similar or larger communication range.[7]
Business Application Identifier (BAI)		Two-character code that identifies the intended use of a push payment. It determines the data carried in the message, the limits and economics that may apply to the transaction, and may be used by the sending and/or receiving issuer to make an authorization decision.[8]
Card Not Present (CNP)		Payment card transaction where the cardholder does not present the card for merchant examination at the time of purchase, such as a mail-order transaction or a purchase made over the telephone or Internet (using the U.S. Payment Forum CNP white paper definition[9]). *Mobile-based payments create complexities relative to card-present and card-not-present payments.[9]
Card On File		Payment credentials provided by the cardholder to a merchant with the authorization to use the stored "card on file" credentials for payment (for individual or recurring payments).[10]
Cardholder Initiated Transaction		Any transaction where the cardholder is present and provides their payment credential. This can be through a terminal in store or online through a checkout experience. A cardholder-initiated transaction contains verification that the cardholder was involved in the transaction.[5]
Closed Loop Mobile Payment		A mobile payment system that is specific to single merchant organization or small group of merchants.[11]
Cloud		A reference to using cloud computing to access services and applications. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]

Term	Also Known As (AKA)	Industry Stakeholder Definition
Consumer Device Cardholder Verification Method (CDCVM)	On-Device Cardholder Verification Method (ODCVM)	A method that uses a mobile payment device (e.g., phone, wearable, card) to authenticate cardholder identity in a mobile payments transaction (e.g., PIN or biometrics).[1]
Contactless Chip Card		A chip card that communicates with a reader through a radio frequency interface. Communication is defined by ISO 14443.[2]
Contactless EMV Payment		An EMV chip payment transaction that uses the contactless interface of a chip card and communicates with an EMV chip-enabled reader using radio frequency and results in an EMV cryptogram.[1]
Contactless Payments		Payment transactions that require no physical contact between the consumer payment device and the physical terminal. In a contactless payment transaction, the consumer holds the contactless card, device, or mobile phone in close proximity (less than 2-4 inches) to the terminal and the payment account information is communicated wirelessly (via radio frequency [RF]) or NFC.[2]
Contactless POS Terminal/Reader		A terminal/reader with contactless functionality, enabling it to accept contactless payments, including payments from contactless magnetic stripe mode and contactless EMV enabled devices (e.g., chip cards and mobile NFC devices that are provisioned with payment applications and credentials).[1]
Data Encryption Standard (DES)		A cryptographic algorithm adopted by the National Bureau of Standards for data security. Encryption scrambles personal identification numbers (PINs) and transaction data for safe transmission.[20]
Digital Wallet	eWallet	A software representation of a physical wallet. For example, putting debit and credit cards into an application that holds payment credentials through which someone can pay, using the digital version of the debit or credit cards in that person's physical wallet, linking to the same account, to pay.[20]
Dual-Interface Card		A chip card that allows the chip to be accessed by both the contact plate on the card and the antenna embedded in the card.[1]
Dual-Interface POS Terminal		A terminal with both EMV contact and contactless functionality. If enabled, payment transactions can use either interface. Notes: "Hybrid" terminals accept contact and magnetic stripe only. It does not include contactless.[20]
Dynamic Card Verification Value/Code	dCVV, dCVC, dCVx	Dynamic CVV/CVC, allows the issuer to secure contactless MSD mode transactions by allowing the contactless card to generate a dCVC/dCVV using a diversified key and then include the dynamic card verification value/code in the discretionary data field of the track data which will allow the issuer to verify the secure contactless MSD mode transaction. The different payment networks' contactless specifications use different dynamic data to secure the contactless MSD mode transaction.[9]
Embedded Secure Elements		An embedded, fixed and therefore non-removable separate secure chip in the mobile phone.[1]

Term	Also Known As (AKA)	Industry Stakeholder Definition
Enrollment		The process of registering an account (e.g., payment or loyalty accounts) into a mobile or e-wallet.[20]
Facial Recognition		Biometric method that requires a device to view an image or video of a person's face and compare it to an image or video in a reference database. The comparison examines the facial structure, shape, and proportions; the distance between the eyes, nose, mouth, and jaw; the upper outlines of the eye sockets; the sides of the mouth; the location of the nose and eyes; and the area surrounding the cheek bones. Could be used for cardholder verification.[20]
Fingerprint Recognition		Biometric recognition based on unique characteristics gleaned from impressions of the ridge valley patterns (e.g., ridge flow, ridge spacing, ridge endings, ridge bifurcations) present on human fingers. Could be used for cardholder verification.[20]
Geofence		A geographic zone that is defined for tracking purposes. When a tracking device in a vehicle or a person with a smartphone tracking app enters or leaves a geofence, the device sends a signal via e-mail or texting to a recipient. Geofences can be permanently assigned or temporary.[13]
Geolocation		The physical location of an object in the world, which may be described by degrees of longitude and latitude or by a more identifiable place such as city or residence. Being able to identify the location of a user via the geolocation methods in a smartphone (e.g., GPS, cellular) has enabled entirely new applications and businesses.[14]
GPRS or (General Packet Radio Service)		The first high-speed digital data service provided by cellular carriers that used the GSM technology. GPRS added a packet-switched channel to GSM, which uses dedicated, circuit-switched channels for voice conversations.[1]
GSM		A European Telecommunications Standards Institute (ETSI) standard for digital cellular phones that use integrated cards for identification and security.[20]
GSMA		GSM Association: Association of about 700 mobile network operators (MNOs) in 218 countries around the world.[1]
Host Card Emulation (HCE)		HCE is mechanism for an application running on the "host" processor (the mobile device's main processor–where most consumer applications run) to perform NFC card emulation transactions with an external reader. Examples of HCE implementations include the Android operating system (Android KitKat 4.4 and higher) and the BlackBerry operating system.[20]
In-App Payment		*In-app* refers to making a mobile purchase from within a mobile app. There is a distinction between paying with NFC mobile wallets and paying directly through the merchant-specific *native* mobile app with credit, debit or prepaid card number, typically stored in a digital wallet.[20]
Interaction Method for Proximity Payments		The technology used to communicate wirelessly between a payment device and a POS terminal. Technologies used include: NFC; ISO/IEC 14443 (for cards); QR code or bar code; BLE.[18]

Term	Also Known As (AKA)	Industry Stakeholder Definition
ISO/IEC 14443		ISO/IEC standard "Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards." The international standard for contactless chips and chip cards that operate (i.e., can be read from or written to) at a distance of less than 10 centimeters (4 inches). This standard operates at 13.56 MHz.[1]
ISO 18004		ISO/IEC 18004. Information technology—automatic identification and data capture techniques—QR code bar code symbology specification.[20]
ISO 18092		ISO/IEC 18092:2013 defines communication modes for near field communication interface and protocol (NFCIP-1) using inductive coupled devices operating at the center frequency of 13,56 MHz for interconnection of computer peripherals. It also defines both the active and the passive communication modes of NFCIP-1 to realize a communication network using NFC devices for networked products and also for consumer equipment. ISO/IEC 18092:2013 specifies, in particular, modulation schemes, codings, transfer speeds, and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization. Furthermore, ISO/IEC 18092:2013 defines a transport protocol including protocol activation and data exchange methods.[4]
Limited Use Payment Credential (LUPC)	Limited Use Token	Payment credential that is provisioned to a mobile device that is single use or only usable for a specific purpose or time.[15]
Loyalty Front End Processor (LFEP)	Loyalty Host, Mobile Financial Service Provider	This entity is a host that facilitates the authorization of loyalty rewards, including rewards issued or redeemed using a mobile device. The LFEP entity is sometimes referred to as the loyalty host. There may be multiple LFEPs involved in processing a single transaction. Note: ISO 12812 would treat an LFEP that issues a loyalty app that affects a final transaction amount as a mobile financial service provider (MFSP).[20]
Magnetic Secure Transmission (MST)		A proprietary technology implemented in certain mobile phones that uses RF to communicate payment account information with a magnetic-stripe reader of a POS terminal.[1]
Magnetic Stripe Data (MSD) Transaction		A contactless payment transaction that transfers data that is formatted as the magnetic stripe of a credit or debit card.[1]
Merchant Initiated Transaction		An authorization request that relates to a previous cardholder-initiated transaction but is conducted without the cardholder present, and without any cardholder validation performed.[5]
Mobile Check-In		The process whereby people use their mobile device to indicate and/or register their arrival at a place or event.[19]
Mobile Coupons		An electronic offer entitling the holder to a discount, free gift or some other form of marketing promotion to encourage commerce with the issuer of the offer.[1] *May be independent or combined with a mobile wallet.
Mobile Loyalty		A mobile implementation of a loyalty program.

Term	Also Known As (AKA)	Industry Stakeholder Definition
Mobile Marketing		As defined by the Mobile Marketing Association, a set of practices that enables organizations to communicate and engage with their audience in an interactive and relevant manner through any mobile device.[1]
Mobile Network Operator		Provider of wireless communications services that owns or controls all of the elements necessary to sell and deliver services to a user, including radio spectrum allocation, wireless network infrastructure, back haul infrastructure, billing, customer care, provisioning computer systems, and marketing and repair organizations.[9]
Mobile Offers		Similar to a mobile coupon, a mobile offer is intended to communicate awareness of a product or service to the receiver and ultimately would drive engagement with the issuer in terms of product or service purchase.[1]
Mobile Payment Application (MPA)		This entity is a software application installed to a mobile device which enables mobile payment transactions. The application may locally store payment card data and non-payment card data (e.g., loyalty, purchase history) required to complete the transaction. The payment card data may also be stored in a token vault or by a token/trusted service provider. In addition, the mobile payment application will be responsible for geo-location functionality.[20]
Mobile Payment Provider		Entities providing a means of acceptance to the merchant for mobile payment services.[20]
Mobile Payment Provider Application (MPPA)	MPS (Mobile Payment Server)	A cloud-based application provided by the mobile payment processor (MPP) responsible for interfacing between the token vault or token/trusted service provider, the MPA, the site system and the payment front end processor (PFEP) in order to authorize transactions.[20]
Mobile Payment Device		This term can be both broadly and specifically defined. The broad use could be a device that supports payment, including wearables, both with passive power or battery powered sources. Specifically, most common examples include smartphones and tablets.[20]
Mobile Point-of-Sale (mPOS)		Mobile point-of-sale (mPOS) acceptance solutions allow merchants to use mobile devices as point-of-sale terminals to facilitate payment transactions. mPOS acceptance solutions typically make use of a "mPOS card reader accessory" that can either be plugged into the audio jack or USB port or connected via Bluetooth to read magnetic stripe, contact chip or contactless payment cards. "Mobile devices" refer to consumer oriented, multi-purpose mobile computing platforms, including feature phones, smartphones, tablets, and PDAs.[20]
Mobile proximity payments		Mobile payment transaction in which a consumer uses a phone to pay for goods or services at a physical POS.[1] Payment credentials are transmitted from the mobile device to the physical POS.

Term	Also Known As (AKA)	Industry Stakeholder Definition
Mobile Remote Payments		Mobile payment transactions in which consumers use a mobile device to make purchases without interacting with a physical POS.[1] The payment credentials are not obtained by the POS off the mobile device.
Mobile Wallet		The mobile version of a digital wallet, provisioned and accessed on a mobile device.[20]
Near Field Communication (NFC)		NFC is a set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, personal computers or wearable devices. An NFC-enabled mobile device can communicate with a POS system that currently accepts contactless payment cards.[1]
NFC-Enabled Mobile Device		A smartphone, tablet or wearable that supports NFC.[1]
One-Time Password (OTP)		Passwords that are used once and then discarded. Each time the user authenticates to a system, a different password is used, after which that password is no longer valid. One-time passwords are often delivered to the user via one of the following methods: text or e-mail, display card, or RSA token.[1]
Open Loop Mobile Payment		A mobile system that uses open loop payments. This is in contrast to a closed loop payment scheme.[20]
Optical Reader		A camera on a mobile or a point of sale device that can recognize and extract information such as from a QR code, physical card, or bar code.[20]
Over the Air (OTA)		The possibility to send and receive data to/from a device in distributed environment. In GSM networks, data connection or SMS could be used to do so.[1]
Pass Through Wallet		A mobile wallet that provides all the information a normal checkout would require directly to the POS or app.[16]
Payment Account Reference (PAR)		A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to its affiliated payment tokens.[1]
Payment Front End Processor (PFEP)	FEP, Acquirer, Acquiring Processor, Payment Host, Mobile Financial Service Provider	The application or institution that the merchant location uses for the processing of payments. This may be a third party provided application made available as a service or an in-house application provided by the MPP.[3] Note: ISO 12812 would treat a PFEP as a mobile financial service provider (MFSP).
Payment Service Provider (PSP)		Non-bank service providers (e.g., providers of technology, software, network services, processing services, mobile wallets, equipment, security services, program managers).[18]

Term	Also Known As (AKA)	Industry Stakeholder Definition
Point-of-Sale (POS)		The device (hardware and software) that is used to process transactions on the merchant location.[3] While POS once referred specifically to the credit card terminal at the cash register, POS now includes mobile, wireless, and virtual terminals.[20]
Provisioning		An initial set up process that handles authentication of a user account, the exchange of keys to unlock the NFC chip installed on a mobile device, the service activation and the secure download of mobile payment account information.[20]
Pull Payment		A payment made after prior authorization by the payer; the payee sends the payment instruction to the payee's account to draw on funds from the payer.[12]
Push Payment		A payment made when the payer sends the payment instruction to the payer's account to transfer the payer's funds to the payee.[12]
QR Code		Quick response code. A type of 2-D (matrix) bar code that complies to ISO 18004:2006.[21]
Radio-Frequency Identification (RFID)		Technology that is used to transmit information about objects wirelessly, using radio waves. RFID technology is composed of 2 main pieces: the device that contains the data and the reader that captures such data.[1]
Secure Element (SE)		The secure element resides in a microcontroller chip capable of performing cryptographic operations. It offers a dynamic environment to store data securely, process data securely and perform communication with external entities securely. If tampered with, it may self-destruct, but will not allow unauthorized access.[20]
SIM **Subscriber Identity Module**	SIM Card, Subscriber Identification Module	The smart card that is included in GSM (Global System for Mobile Communications) mobile phones. SIMs are configured with information essential to authenticating a GSM mobile phone, thus allowing a phone to receive service whenever the phone is within coverage of a suitable network.[1]
Site System		This term encompasses the site equipment and components (hardware and software) physically present at the merchant location. It may perform the function of local card processing business rules such as customer prompting, local velocity checking and receipt formatting and printing. Examples of site systems include point of sale (POS) and electronic payment server (EPS).[3]
Short Message Service (SMS)		A system used to send text messages to and from mobile phones.[1]
Staged Wallet		A mobile wallet that draws down the funds spent by their customers from a payment card or account that has been pre-linked to the consumer's digital or mobile wallet. Example: PayPal.[17]
Store and Forward	Deferred Authorization	Refers to transactions when a merchant captures transaction information and transmits after transaction completion for subsequent processing.[20]

Term	Also Known As (AKA)	Industry Stakeholder Definition
Token		Generic term for a placeholder or surrogate. In the context of payment card transactions, a token refers to a surrogate card number that is submitted in the payment stream in place of the real card number.[20]
Token Requestor		Entity that initiates requests that PANs be tokenized by submitting token requests to the token service provider.[20]
Token Service Provider (TSP)		Entity within the payments ecosystem that provides registered token requestors with 'surrogate' PAN values, otherwise known as payment tokens by managing the operation and maintenance of the token vault, deployment of security measures and controls, and registration process of allowed token requestors.[20]
Token Vault		A secure Payment Card Industry (PCI) compliant server where issued tokens, and the PAN numbers they represent, are stored securely.[20]
Tokenization		Process by which a placeholder or surrogate (payment token) is substituted for a primary account number. Typically, tokenization is a service offered by a payment network, acquirer, token service provider or third party service provider.[9]
Trusted Execution Environment (TEE)		A TEE is an execution environment that runs alongside the smartphone operating system (the rich OS). A TEE provides security services and isolates access to its hardware and software security resources from the rich OS and associated applications.[22]
Trusted Service Manager (TSM)		A neutral third party that provides a single integration point to mobile operators for financial institutions, transit authorities and retailers that want to provide a payment, ticketing or loyalty application to their customers with NFC-enabled phones.[1]
USIM-Based Cards		The equivalent of a SIM card in WCDMA/UMTS (3G) phones.[1]
Wallet Service Provider		Companies that offer specific wallet solutions that use various communications technology for mobile payments.[23]
Wearable		In the context of payment: relating to or noting a computer or advanced electronic device that is incorporated into an accessory or item of clothing worn on the body.[24]
Wireless Application Protocol (WAP)		A global application protocol that enables mobile phone users to access the Internet and other information services.[1]

4. Legal Notice

While great effort has been made to ensure that the information in this document is accurate and current, this information does not constitute legal advice and should not be relied on for any legal purpose, whether statutory, regulatory, contractual or otherwise. All warranties of any kind are expressly disclaimed, including all warranties relating to or arising in connection with the use of or

reliance on the information set forth herein. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk.

Nothing in this document constitutes or should be construed to constitute an endorsement or recommendation of any particular approach, service or provider, and all implementation decisions and activities should be properly reviewed in light of applicable business needs, strategies, requirements, industry rules

All registered trademarks, trademarks, or service marks are the property of their respective owners.