SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE PAYMENTS COUNCIL WHITE PAPER

Contactless Payments: Proposed Implementation Recommendations

Version 1.0

January 2018

Secure Technology Alliance
191 Clarksville Road
Princeton Junction, NJ 08550

www.securetechnologyalliance.org

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

Table of Contents

1 Introduction

We live in a rapidly evolving digital world—a world in which consumers are usually connected. This increased connectivity is altering consumer expectations. Consumers now want payment to be faster, more secure, and seamless. Issuers can meet these changing expectations by offering contactless payments.

Merchants can benefit from the growth of digital commerce by preparing to accept digital payments across channels—through e-commerce, via in-app payment, and at the point-of sale (POS) using contactless payment. Contactless payment brings multiple benefits to merchants, including faster checkout, increased transaction volumes, higher consumer spending, and reduced cash handling costs. Contactless also enables a new generation of mobile payments. Contactless payment is particularly applicable to high-throughput low-value retail environments, where cash is currently the predominant payment method. For such merchants, adding contactless capability through terminal upgrades or simple plug-in devices makes sense.

This white paper focuses on some of the key recommendations for implementing contactless and Near Field Communication (NFC)-enabled form factors (such as cards, mobile phones, rings, and key fobs) and POS acceptance devices in the North American market. The white paper does not discuss the security of contactless transactions.[1] Where relevant, the paper provides implementation recommendations and suggests industry contacts with whom to engage to implement contactless payments successfully.

[1] For a detailed discussion of security, see Secure Technology Alliance, "Contactless Payment Security Questions & Answers," https://www.securetechalliance.org/wp-content/uploads/Contactless-Payments-Security-QA-FINAL-Dec-2016.pdf.

2 Contactless Acceptance: Merchants

Many U.S. merchants have already implemented EMV contact chip card solutions. Merchants who are thinking about implementing contactless payments should consider the following:

- Testing and certification
- Contactless acceptance terminals
- Cardholder experience with different contactless form factors
- Employee training
- Contactless payment devices in the market
- Implementation priorities
- Mobile contactless payment implementation

2.1 Testing and Certification Requirements

Deploying a contactless solution requires both hardware and software testing and certification.

2.1.1 Deployment Prerequisites

Before deploying a contactless solution, merchants are required to have the following:

- Contactless Level 1 and Level 2 letters of approval (LOAs) from the relevant payment networks.
- A valid (unexpired) LOA.

  Global Payment networks may support testing on an expired EMVCo approved kernel for a year from the expiration date of the kernel. Refer to each payment network for details on their processes.
- If the merchant terminal supports PIN entry, a PCI-compliant pin entry device (PED).
- A contactless test tool to perform acquirer Level 3 terminal certification and internal integration and systems testing.

  Chip test tools are available from any test tool provider accredited by the payment networks.

Some payment networks may also require a terminal quality management statement to verify the terminal configuration.

The acquirer performs the Level 3 certification, which is end-to-end testing with each of the payment networks.

2.1.2 Required Certifications

Terminal manufacturers should obtain EMVCo Level 1 (hardware) and Level 2 (kernel) certification for the POS terminal from EMVCo or the appropriate payment networks. Each payment network has terminal testing requirements for acquirer certification of the contactless POS application to confirm that the application, kernel, and processing platform meet payment network product-related requirements. This testing is performed during Level 3 certification with the acquirer.

Use of the EMV contact and contactless interfaces requires a separate Level 3 terminal certification for each unique interface. Each certification imposes a unique set of test cases, based on the environment and products that the contactless terminal supports.

Only one Level 3 contactless certification is necessary for each global payment network if the terminal operating system, POS payment application, kernel, and terminal-to-acquirer message format are the same. The global payment networks' testing and certification requirements also recognize a terminal "family" (i.e., the same operating system, contactless kernel, and POS application are used throughout the merchant's implementation); in this case, only a single certification is required for that family.

Unlike contact EMV, each global payment network has their own contactless kernel which complicates the documentation requirements, but does not necessarily add complexity to the Level 3 certification. Details regarding contactless testing and certification can be found in the U.S. Payments Forum white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community."[2]

2.1.3 Testing Best Practices

Testing is fundamental. It limits potential interoperability issues and saves time and money during deployment. The following best practices are key to successful testing and certification:

- Work with your acquirer to include testing in the overall project plan.
- Determine test requirements based on terminal capabilities, configuration, and merchant environment.
- Conduct internal testing unique to your environment.
- Identify tools that fit your testing needs.
- Identify dedicated resources with EMV knowledge. Using such resources can save time by minimizing the number of test cycles.
- Minimize unnecessary retesting by isolating the payment application from other software changes.
- Use standardized solutions to reduce the number of solutions that need to be tested or deployed in same terminal family.
- Modularize and isolate EMV functionality by using semi-integrated solutions.

2.1.4 Recommendations

Testing and certifying contactless technology is similar to the process that was followed for EMV contact. Merchants should contact their testing partners or networks to obtain further information on testing and certification.

Faster EMV solutions (i.e., Quick Chip and M/Chip Fast) operate across payment networks, support contactless payments, and could also reduce the scope of testing and certification.[3]

---

[2] http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/.

[3] For more detail, see the U.S. Payments Forum white papers, "Optimizing Transaction Speed at the POS," Oct. 2017, http://www.emv-connection.com/optimizing-transaction-speed-at-the-point-of-sale/ and "EMV Testing and Certification White Paper: Current U.S. Payment Brand Requirements for the Acquiring Community," http://www.emv-connection.com/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/.

2.2 Contactless Acceptance Terminal Considerations

Contactless payments are not new. Contactless payments relying on magnetic stripe data (MSD) have been available since 2005. However, as the U.S. transitions to EMV, some payment networks are no longer recommending contactless MSD solutions. Moreover, some EMV contactless cards are being deployed without contactless MSD support, which can cause interoperability issues or cause a transaction to be terminated and processed using the EMV chip or magnetic stripe.

2.2.1 MSD Contactless vs. EMV Contactless: Support Issues

If a merchant's POS terminal supports only MSD contactless, processing issues may arise with contactless transactions at the POS. While mobile wallets are generally backward compatible with MSD, cards and wearables may support only EMV contactless transactions. This incompatibility can result in a technology mismatch at the POS—the contactless antenna in the terminal detects a contactless card, but the POS application is unable to process the data from the chip. The result is that incorrect transaction data may be sent to issuers, leading to lower approval rates than for EMV contactless transactions.

Additionally, in the rare situation where the antenna on the contactless POS terminal and the magnetic stripe reader are in close proximity, a contactless transaction may be unintentionally initiated when a consumer is intending to do a magnetic stripe transaction. If the merchant has not yet implemented EMV contactless, the result is an error and delay at the POS. This issue may be resolved by ensuring the terminal hardware and software capabilities are configured to current best practices.

Table 1 indicates how transactions are handled in different situations based on the capability of the terminal and card or device.

Table 1. How Contactless-Capable Cards Interact with Contactless-Capable Terminals

Card or Device Capability		Terminal Capability		
MSD	**EMV**	**MSD**	**EMV**	**Payment Transaction**
X	X	X[b]	–	MSD contactless
X	X	X	X	EMV contactless
X	X	–	X	EMV contactless
–	X	X[b]	–	Transaction may be terminated and processed as a contact chip or magnetic stripe transaction
–	X	X	X	EMV contactless
–	X		X	EMV contactless
X[a]	–	X [b]	–	MSD contactless
X[a]	–	X	X	MSD contactless
X[a]	–	–	X	Transaction may be terminated and processed as a contact chip or magnetic stripe transaction

[a] Only limited numbers of MSD-only devices are expected to be in the market.

[b] The majority of terminals are currently MSD-only terminals; the number is expected to decline as merchants implement EMV contactless.

Most POS terminals manufactured over the last few years have included EMV-capable hardware, which includes support for contactless EMV. Merchants with newer POS terminals will not need external contactless reader hardware, reducing complexity and integration issues.

However, the contactless infrastructure is still more complex than contact. Contactless terminals require an antenna, which may be different on different terminals due to the varying physical characteristics of each contactless terminal model. Small countertop or mobile POS terminals must have a different antenna than larger multilane devices. These POS terminals are generally backward compatible, supporting both MSD and EMV contactless, but software and payment system infrastructure changes are also necessary to add EMV support to an MSD-only contactless terminal.

2.2.2 Terminal Capabilities Settings

Contactless terminals typically have capability settings that are maintained through configuration files that can be downloaded from either the merchant POS host or the merchant services provider. It is crucial that these settings reflect only the capabilities for which the terminal is certified or approved. For example, if a terminal does not contain an approved or certified contactless application, the contactless capability should not be enabled. If the application is approved for MSD contactless but not EMV contactless, the capability settings should reflect that restriction. If a merchant updates the terminal to include a certified EMV contactless application, the terminal capability settings should also be updated. Inaccurate capability settings can result in acceptance issues at the POS and customer dissatisfaction.

In addition, authorization request messages should accurately reflect these capabilities, according to the merchant acquirer/processor's message specification. Mismatches between actual and reported capabilities can lead to data quality issues and processing errors.

2.2.3 Enabling Contactless POS Terminals

While several issues must be considered when enabling a contactless terminal at checkout, one of the most important is location. Terminals must be customer facing and not close to any electrical equipment or metal objects that could create interference.

To determine appropriate locations, merchants should examine the establishment's floor plan carefully, with the assistance of the acquirer. If different sites have different floor plans, examine each one separately, taking into account such considerations as the location of electrical outlets, the amount of counter space available, and the location of data ports. Certain sites may present unique challenges—such as the location of underground conduits for drive-through solutions or special cabling requirements for reader integration with standard terminals. One size may not fit all.

Figure 1 summarizes the best practices for enabling a contactless terminal at checkout.

2.2.4 Recommendations

Upgrading to EMV contactless is the surest way to ensure card and terminal interoperability, both within the U.S. and globally. Upgrading also supports better security (EMV-strength cryptograms) and additional functionality (new cardholder verification methods).

Upgrading to EMV contactless is also the surest way to ensure that terminal settings are proper, and that data is of the highest quality, since thorough testing and certification is a prerequisite to the upgrade. An EMV contactless upgrade is incremental, since the majority of the terminal hardware deployed is EMV capable and similar testing processes to EMV contact are available.

Follow best practices for enabling contactless POS terminals in stores. Merchants should consult with their terminal provider for additional guidance on terminal installation recommendations and requirements.

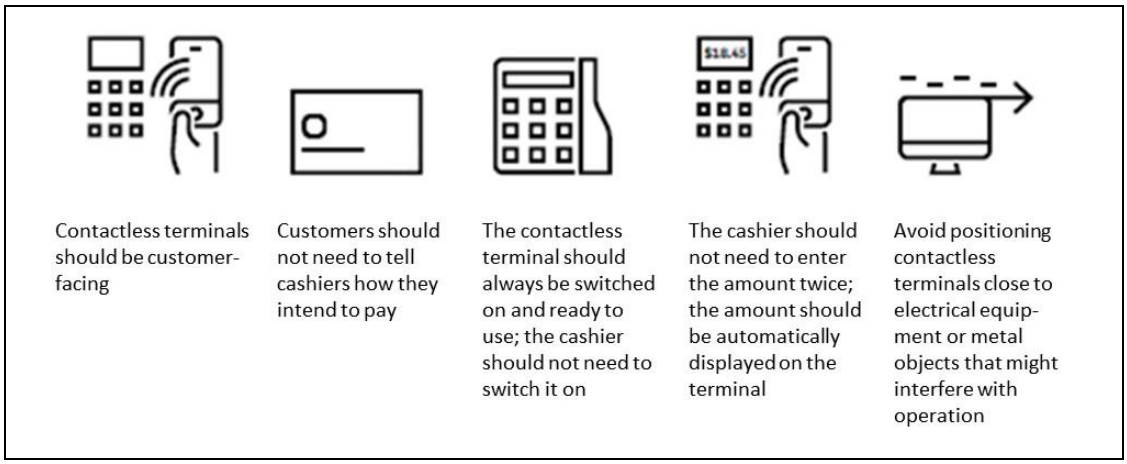


Figure 1. Enabling a Contactless Terminal at the Checkout

2.3 Cardholder Experience: Different Contactless Form Factors

When performing contactless transactions, consumers already use a variety of form factors—contactless cards, mobile wallets on phones, wearables (such as watches, rings, or key fobs)—and there may be additional options in the future. While the "tapping" procedure to initiate the transaction should be the same regardless of form factor, other consumer behavior may not be consistent, especially when using a wallet on a mobile phone. Transactions initiated using a mobile phone involve a two-step process: first, the wallet is activated (using an authentication method such as a biometric,[4] PIN, or pattern); second, the phone is placed in proximity to the POS device for the contactless read.

Generally, however, the authentication mechanism used as the cardholder verification method (CVM) will be the consumer device cardholder verification method (CDCVM). CDCVM uses a mobile phone's passcode or biometric user authentication to verify the cardholder for a payment transaction, removing the need for the cardholder to enter a PIN or provide a signature. Such use can result in an inconsistent consumer experience; sometimes a cardholder may be required to provide a PIN or signature on the terminal (for example, if the contactless terminal does not support CDCVM) and sometimes no verification will be required. However, as consumers become more familiar with the process and as older terminal functionality is replaced with newer technology, there should be fewer inconsistencies. In addition, note that, at this time, some networks may not support CDCVM with their U.S. common debit AID, which may result in inconsistent consumer experience for debit transactions.

2.3.1 Recommendations

While the cardholder experience when performing contactless transactions is not completely consistent, the same has always been true for other forms of electronic payments. Issuers, merchants, and networks have developed ways to tell consumers how to make a particular payment work. Contactless

[4] Mobile phones support different biometric technologies that may be used for authentication, including fingerprints, voice recognition and facial recognition.

will be no different. Merchants should train staff to understand that there are a variety of CVMs that may be used with contactless and capture the required data as requested by the terminal.

2.4 Employee Training

Training is one of the most critical aspects of successful contactless implementation. It is extremely important that cashiers and other staff understand how contactless payments are processed and what the differences are between contactless and traditional payment methods.

Cardholders receive use instructions when they receive their contactless cards. However, merchants should ensure that their cashiers understand how to operate the contactless terminals and are able to assist a cardholder. Incidents have been reported in which cashiers were unaware that the terminal included contactless capability or, while familiar with mobile wallets, were unaware of contactless cards.

In addition to mobile wallets and cards, contactless payments can be made using form factors such as watches, rings, and other wearables. Some wearables may not require cardholder verification, while others may if the transaction exceeds the cardholder verification limit. For these form factors, the cashier will not be able to verify a signature when prompted, although the issuer will be able to verify the online PIN or determine whether the CDCVM was verified successfully.

Employee training that instills employee confidence in the technology and encourages use by customers is critical to a successful deployment. Training must be consistent and ongoing, so that employees know how to use their contactless acceptance devices and can explain their use to customers. Employees should also learn to prompt customers to use their contactless-enabled payment devices, to encourage activation and usage.

2.4.1 Key Topics for Training

Training should cover these key topics:

- Variety of form factors. Contactless payments are available to consumers in a variety of form factors, including cards, key fobs, stickers, wearables (e.g., watches, rings, fitness trackers) and mobile phones.
- Identification. A card or other form factor is identified as contactless by a contactless indicator. There should also be a contactless indicator on the screen of any contactless-capable mobile device and a contactless symbol on the contactless POS terminal (Figure 2).
- Cardholder verification. Contactless is ideal for low-value payments with no CVM; however, like contact card transactions, higher value transactions may require cardholder verification using a signature, PIN, or CDCVM.
- Security. Some customers will be nervous about the security of contactless payments. Employees should understand why contactless is highly secure so that they can reassure customers.[5]
- Signage. The most effective merchants display POS collateral that lets customers know that contactless payments are accepted. Consider including information about contactless

[5] Additional information on contactless payments security can be found in the Secure Technology Alliance publication, "Contactless Payment Security Q&A," https://www.securetechalliance.org/publications-contactless-payment-security-qa/.

acceptance in marketing and advertising materials to help build awareness of contactless payments, encourage use, and strengthen customer satisfaction.

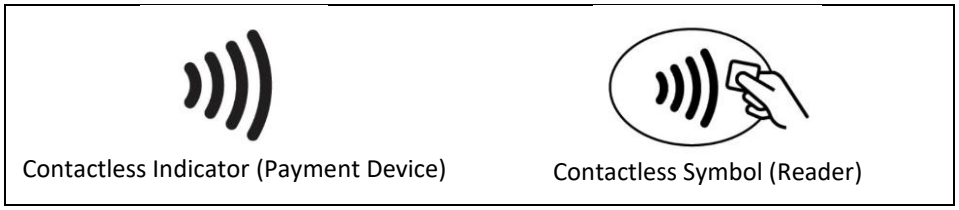


Figure 2. Contactless Indicator and Contactless Symbol

2.4.2 Best Practices for Training

Effective training should incorporate the following best practices (Figure 3):

- Create appropriate training programs for employees and store managers.
- Keep training current with refresher training, to keep employees engaged and to train new employees.
- Consider "train the trainer" programs.
- Teach employees to promote contactless transactions, as advocates and educators.

Figure 3. Best Practices for Training

2.4.3 Recommendations

Follow best practices for training staff. Training materials developed for other "contactless mature" markets can also be leveraged. The need for training diminishes as contactless adoption increases, since merchants will see more contactless devices and consumers will become more accustomed to using the different form factors.

2.5 Contactless Payment Devices in the Market

To date, the absence of a critical mass of contactless-enabled cards and the lack of consumer demand has been an inhibitor to merchants upgrading their terminals to support contactless payment. However, several current market trends may help drive contactless demand.

- The introduction and adoption of Apple Pay, Google Pay,[6] and Samsung Pay are driving interest in contactless payments using NFC-enabled mobile devices.
- Issuers are now moving to the next wave of EMV chip card issuance; their adoption of dual-interface chip cards, capable of both contact and contactless transactions, should further stimulate consumer usage.
- Contactless payments reduce card–terminal interaction times, alleviating consumer and merchant frustration with the real or perceived longer transaction times associated with contact chip transactions.
- A growing percentage of merchants have enabled contactless or already have a contactless-capable terminal. For example, Visa has reported that, as of September 2017, 40% of U.S. face-to-face Visa transactions today occur at contactless-enabled locations, indicating that a growing percentage of merchants are enabling contactless.[7]
- The U.S. transit industry is moving to upgrade transit points-of-entry to accept contactless payment cards or devices. As has been demonstrated in London, transit contactless payments drive "top of wallet" consumer behavior and increase use at contactless-enabled merchants located close to transit stations.[8] Transit is sometimes talked about as one of the few merchant verticals where the customer (cardholder), by the definition of being commuters, ride (and pay at a transit POS) 2-3 times a day.

2.5.1 Recommendations

According to Visa, 72 percent of cardholders prefer contactless cards to contact chip cards.[9] The advantages of contactless at the POS and the market trends listed above should provide merchants with the justification to enable EMV contactless as use of contactless-enabled cards and devices grows.

2.6 Merchant Implementation Priorities

EMV acceptance continues to grow, both as a percentage of chip-on-chip transactions and total terminal deployments. While EMV support at the terminal is optional, merchants that choose to remain on the sidelines will continue to be liable for fraud, as defined in the payment network liability shifts.[10] Additionally, there is no requirement that EMV contactless must be supported.

Today, U.S. EMV contact card issuance has reached a saturation point. As U.S. EMV card issuance matures, cards are expected to support both the contact and the contactless interfaces. Coupled with

---

[6] Google, "Bringing it all together with Google Pay," Google blog post, January 8, 2018, https://www.blog.google/topics/shopping-payments/announcing-google-pay/. Google announced that they are bringing together all the different ways to pay with Google, including Android Pay and Google Wallet, into a single brand: Google Pay.

[7] Visa, "Contactless in the U.S.," October 2017

[8] "Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers," Secure Technology Alliance white paper, June 2016, https://www.securetechalliance.org/publications-contactless-emv-payments-benefits-for-consumers-merchants-and-issuers/.

[9] Money 20/20 presentation, Avin Arumugam, Visa, Oct. 24, 2017

[10] Additional information on the U.S. EMV fraud liability shifts can be found in the U.S. Payments Forum white paper, "Understanding the U.S. EMV Fraud Liability Shifts," http://www.uspaymentsforum.org/understanding-the-u-s-emv-fraud-liability-shifts/.

mobile wallet and other contactless form factors, consumers will have many opportunities to embrace contactless payments.

While EMV issuance has reached saturation, merchant EMV acceptance has not kept pace. As merchants develop or progress on their roadmap priorities, contactless support should be considered. For many merchants, initial EMV support is still in progress. Others may be utilizing their first or second (or more) generation EMV application.

Wherever the merchant is at on the EMV roadmap, there are several key considerations:

- Consumers are educated and are expecting merchants to accept EMV chip cards.
- Testing and certification for contact and contactless has been simplified by payment networks, acquirers and acquirer processors.
    - Payment networks have implemented Faster EMV solutions, resulting in an enhanced customer experience at the point of sale and a simplified testing and certification process.
    - Many acquirers and acquirer processors have implemented streamlined processes and tooling.

The combination of these factors has reduced the testing and certification cycle time while improving the customer experience, making it more straightforward for merchants to implement both contact and contactless EMV solutions.

2.6.1 Recommendation

Whether a merchant is embarking on their initial EMV migration or if the payment application is in the process of being upgraded, the merchant should consider implementing EMV contactless.

2.7 Mobile Contactless Payments Considerations

2.7.1 CDCVM Support

One of the features of mobile wallets[11] is the consumer device cardholder verification method (CDCVM). CDCVM uses verification methods from the mobile phone (e.g., passcode or biometric) to provide cardholder verification in the payment transaction. This verification removes the need for the cardholder to provide a PIN or signature when it may otherwise be required (e.g., when the transaction amount is over the contactless "no CVM" transaction limit). As a result, the cardholder payment experience is faster and more seamless.

CDCVM requires support from the contactless kernel, which some older kernels may not include. And adding CDCVM to a previously certified contactless EMV solution may require additional certification.

In October 2016, the FIDO Alliance and EMVCo announced that they are jointly defining use cases and technology standards that will simplify implementation of CDCVM support.[12]

[11] In addition to mobile devices, some new dual-interface interface cards may support CDCVM.

[12] "FIDO Alliance Announces New Authentication Specification Effort with EMVCo to Bring Added Security and Convenience to Mobile Payments," FIDO Alliance press release, Oct. 24, 2016, https://fidoalliance.org/fido-alliance-announces-new-authentication-specification-effort-with-emvco-to-bring-added-security-and-convenience-to-mobile-payments/.

2.7.1.1 Recommendations

Merchants who want to support CDCVM should contact their terminal or POS application provider to determine whether a kernel update is required; their merchant services provider can indicate whether additional testing or certification may be required. Note that some networks may not support CDCVM with their U.S. common debit AID.

2.7.2 EMV Payments Tokenization

Tokenization replaces the primary account number (PAN) with a placeholder or surrogate value (the payment token).[13] The payment networks have implemented tokenization to address the issue of theft and the fraudulent use of PANs. Tokens are replacing PANs in payments made by mobile phone (Apple Pay, Google Pay, Samsung Pay) and other devices to enhance security. Currently, neither contactless nor dual-interface cards use tokens; however, they could be used in the future.

Tokenization involves several key considerations:

- Merchants who rely on PANs for other functions (e.g., loyalty, customer service) will need to consider how to handle those functions without an available PAN.
- Merchants who would like to use tokens should understand the tokenization provisioning and lifecycle management processes and consider the token service providers' identity and verification (ID&V) requirements.
- Merchants, acquirers and processing switches may need to consider the potential impact of extended BIN ranges and tokenization on their routing processes for debit transactions.

The payment account reference (PAR), which is described in the EMVCo tokenization specification,[14] can be used instead of the PAN for certain non-payment use cases.

2.7.2.1 Recommendations

Merchants should review payment network and EMVCo resources on tokenization and consult with their acquirers for guidance on the impact of tokenization.

2.7.3 Wallet Identification

Merchants have expressed a desire to be able to identify which mobile wallet is being used in a payment transaction so that they can use the information for customer service. There is currently no standardized way to identify the mobile wallet being used. However, industry discussions are underway to understand the requirements and explore possible technical approaches.

---

[13] For more information on tokenization, see: EMVCo, "EMV® Payment Tokenisation Specification – Technical Framework," Version 2, Appendix A, Sept. 8 2017, https://www.emvco.com/emv-technologies/payment-tokenisation/; and Secure Technology Alliance, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," October 2014, http://www.securetechalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/

[14] EMVCo, op. cit.

3 Contactless Issuance Considerations

Issuers who are considering contactless payments face challenges unique to their role in the payments ecosystem. Issuers should consider the following:

- Contactless ROI
- Cardholder education
- Contactless POS infrastructure and acceptance
- Issuer processor contactless support
- Open loop contactless payments in transit
- Testing and certification
- Branding considerations for other form factors
- Mobile contactless payment implementation

3.1 Contactless ROI

The financial viability of contactless cards has been proven by the success of dual-interface cards in Canada, the United Kingdom, and Australia, among other places. The data prove that contactless cards displace cash and drive increased transactions ("top of wallet" behavior).[15] For example, Visa has reported that European issuers in 2014-2015 saw 18 percent more transactions after issuing cards with contactless capability.[16]

Unlike other current contactless payment alternatives, such as Apple Pay, Samsung Pay, and Google Pay, contactless cards are controlled by the issuer, so the potential financial benefits to the issuer are numerous. Contactless cards do not depend on third-party apps for functionality. They offer a consistent user experience. The card requires neither a mobile device power source nor a mobile application. Additionally, contactless card technology is mature. Dual-interface cards are already in wide use for payment, while NFC-enabled mobile payments are still getting started.[17]

While there is a cost difference between contactless cards and EMV contact-only cards, as dual-interface delivery volumes are increasing worldwide, costs are decreasing.

3.1.1 Recommendations

If required, engage with your payment network or other trusted sources to help develop the business case for moving to contactless cards or other contactless-capable devices.

---

[15] Secure Technology Alliance, "Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers," Secure Technology Alliance white paper, op.cit.

[16] Visa, op.cit.

[17] For more information on the benefits of deploying contactless cards within the payment ecosystem, see Secure Technology Alliance, "Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers," https://www.securetechalliance.org/publications-contactless-emv-payments-benefits-for-consumers-merchants-and-issuers/, and the infographic, "An Issuer's Guide to Contactless Payments in the U.S.," https://www.securetechalliance.org/publications-contactless-payments-in-the-u-s-guides-for-merchants-and-issuers/.

3.2 Cardholder Education

Effective cardholder education and communication are essential to the success of a contactless launch. To encourage cardholders to activate and use the card or device right away, issuers need to:

- Highlight the benefits of contactless payment.
- Explain how contactless payments work.
- Reassure customers about potential security concerns.
- Provide guidance on where contactless payment is accepted (for example, MasterCard® provides a merchant locator application in most regions).
- Provide customers with consistent, frequent, multiphase marketing.

Issuers should use multiple channels for conveying information, including:

- Effective staff training
- Inserts with card mailers
- National and regional media campaigns
- Marketing initiatives at selected merchants
- Joint programs with network operators or handset manufacturers for mobile payment products

In addition, issuers can create usage campaigns. Motivating contactless-enabled customers to activate and establish the tapping habit can be accomplished through usage incentives such as "tap and receive a promotion."

Markets that have already deployed these cards provide consumers with illustrations of the card being used at the POS. The illustration is included when the card is mailed to the customer. Television commercial campaigns sponsored in conjunction with the payment networks are also an effective tool for educating the public on the proper use of a contactless card. In addition, the card and POS terminal include standard contactless icons that indicate support for contactless transactions.

Figure 4 summarizes how to approach cardholder education.

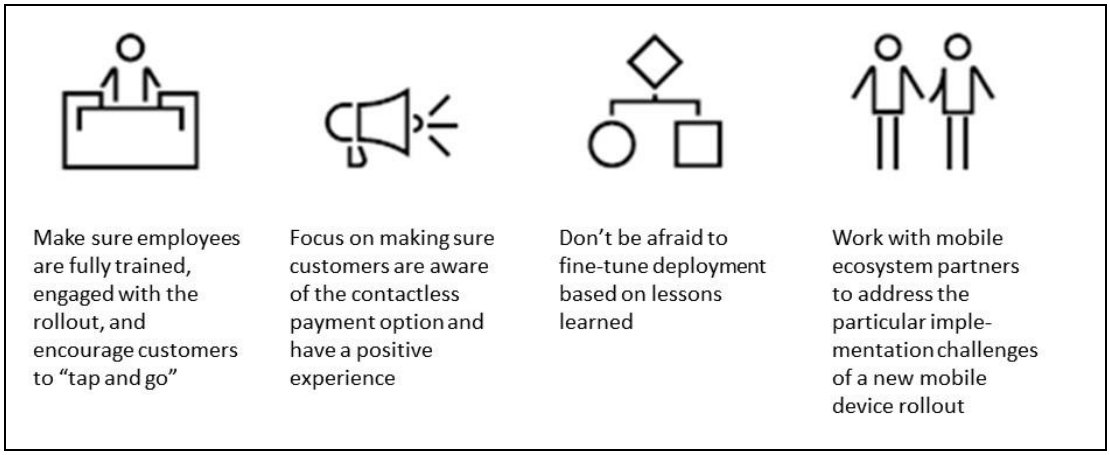
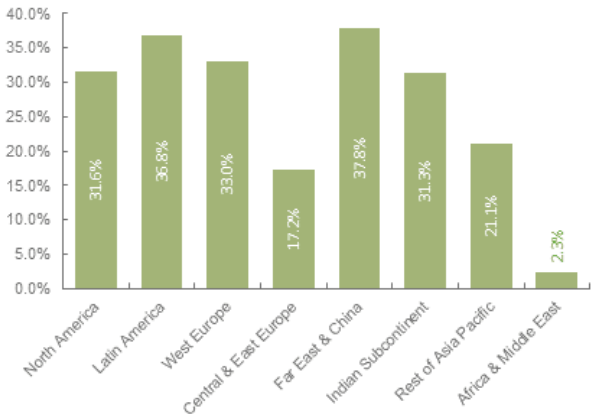


Figure 4. How to Approach Cardholder Education

3.3 Contactless POS Infrastructure and Acceptance

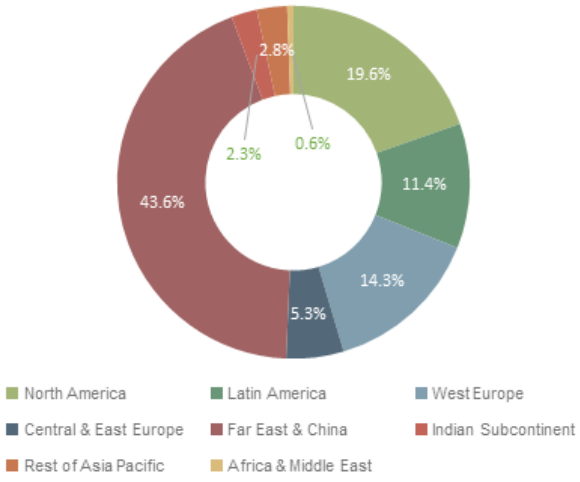
Contactless acceptance is a major trend globally, with a significant percentage of POS terminals supporting contactless. The following are some key published market statistics:

- According to Juniper Research[18] (Figure 5, Figure 6), 31.6% of all terminals in service in North America are contactless; North America accounts for 19.6% of the global installed base of contactless POS terminals.
- Visa has reported that, as of September 2017, 40% of U.S. face-to-face Visa transactions today occur at contactless-enabled locations, that a growing percentage of merchants are enabling contactless.[19]



Source: Juniper Research

Figure 5. Contactless POS Terminals in Service as a Proportion of All POS Terminals (%), End 2016



Source: Juniper Research

Figure 6. Contactless POS Terminals in Service, Regional Share, 2016

[18] Juniper Research: POS and mPOS Terminals 2017-2022

[19] Visa, "Contactless in the U.S.," October 2017

While EMV-enabled POS terminals include EMV contactless capability, legacy MSD contactless terminals still represent a meaningful percentage of the contactless POS infrastructure in the United States. To provide cardholders with the best user experience, issuers should work with the payment networks and card or device personalization vendors to ensure that all EMV dual-interface cards and EMV contactless-capable form factors are backward compatible with MSD contactless terminals.

3.3.1 Recommendation

Merchant support for EMV contactless is expected to increase, as new EMV-capable terminals are installed and contactless device usage increases. Issuers should consider dual-interface EMV cards for the next wave of issuance, to offer their cardholders the benefits of contactless payment while enhancing their brand.

In addition, issuers should consider issuing dual-interface cards that are backward compatible with MSD contactless terminals until the issuer determines that the MSD contactless terminal base has reached an appropriate threshold.

3.4 Issuer Processor Contactless Support

While many issuer processors support contactless, some processors are still updating their platforms to support full EMV contactless, which may affect issuer platform selection. Issuers should consult with their processor to ensure that their platform supports EMV contactless properly.

3.5 Open Loop Contactless Payments in Transit

Transit agencies are moving, or considering moving, to open payments with next generation fare payment systems—that is, credit and debit payments made using contactless EMV devices at transit points of entry (e.g., at fare gates, on buses)— to supplement traditional closed-loop acceptance. As noted in Section 2.5, consumer use of contactless payments for transit can help drive incremental transactions and top-of-wallet status for cards. Issuers contemplating transit as a factor in their contactless decisions should be aware that the specific timing for implementing transit open payments within a given region can have some uncertainty. In addition to the schedule impact of procurement and implementation timeframes, issuers should note that transit agencies interested in open payments may also consider the current state of contactless issuance and other relevant factors in their decision-making process.

Other relevant considerations include the following:

- As the market for open payments in transit is still emerging, the content of the authorization/settlement messages sent from different agency back-end systems may not be consistent.
- Transit merchants may require functionality that addresses transaction times and risk, such as offline data authentication (ODA) and/or deferred (or delayed) authorization.[20]

[20] Additional information can be found in the U.S. Payments Forum white paper, "Technical Solution for Transit Contactless Open Payments Use Case 1: Pay As You Go/Card," http://www.uspaymentsforum.org/technical-solution-for-transit-contactless-open-payments-use-case-1-pay-as-you-gocard/.

The U.S. Payments Forum's Transit Contactless Open Payments Working Committee[21] is developing additional information on transit-specific requirements as part of a resource series, which includes background information on why transit differs from a standard retail merchant environment and functional technical solutions for using contactless form factors to pay for transit.

3.5.1 Recommendations

Issuers should consult with the payment networks about the status of transit open payments initiatives, monitor transit agency programs and plans, and consider participating in ongoing industry dialogue such as the U.S. Payments Forum's Transit Contactless Open Payments Working Committee.

3.6 Personalization Validation

Dual-interface cards require incremental personalization data for contactless, which can be added to an existing contact profile. Personalization validation will ensure that both contact and contactless interfaces function as expected.

3.7 Testing and Certification

Each payment network has a unique contactless application specification that requires payment-network-specific test suites and particular certification processes similar to the EMV contact certification process. Apple Pay, Google Pay, and Samsung Pay NFC contactless payment applications that use tokens require additional testing and certification to ensure that the token and the ISO messaging are handled correctly. Most of the payment networks include mobile form factor testing as part of their profile certification processes.

Contactless also enables new form factors, such as wearables, that may require custom test suites and certification and that may be different for different payment networks. The wearable testing requirements can be addressed by the payment network, card vendor, processor, wearable vendor, or a third-party testing provider. The different form factors will follow the payment network's standard card profile validation process to confirm compliance with the respective brand requirements.[22]

3.7.1 Recommendation

There are existing well-defined testing and certification processes for contactless. Issuers should contact their testing partners or networks for further information on testing and certification.

3.8 Branding Considerations for Other Form Factors

There are currently no branding guidelines for non-card form factors such as wearables. Contact the wearable provider and your payment network partner for further guidance on the branding certification process.

---

[21] http://www.uspaymentsforum.org/working-committees-sigs/transit-contactless-open-payments-working-committee/.

[22] Additional information on payment-enabled wearables can be found in Secure Technology Alliance, "Implementation Considerations for Contactless Payment-Enabled Wearables," October 2017, https://www.securetechalliance.org/publications-implementation-considerations-for-contactless-payment-enabled-wearables/.

3.9 Mobile Contactless Payment Considerations

3.9.1 CDCVM Support

Mobile payment devices perform contactless transactions in accordance with the relevant payment network specifications.

As described in Section 2.7.1, CDCVM enables cardholder verification to be completed using the input and output options on a mobile payment device, with the CVM being verified on the device. The CDCVM can be specific to an individual card. When more than one card is digitized in the mobile payment application, there can be more than one verification method, with different values for each one. Issuers or wallet providers can also use a wallet level CDCVM, where the CDCVM is specific to an individual wallet and all cards stored in the wallet share the same verification method. Another alternative is a device level CDCVM, which shares the CVM method among many applications on the mobile device. For example, the device unlock can be used as a CDCVM. Wallet or device level CDCVMs are referred to as "shared CVMs."

Currently, the U.S. common AID payment application is provisioned onto mobile phones when debit or prepaid cards in the U.S. are digitized into mobile wallets. Some networks may not currently support CDCVM with the U.S. common AID. Issuers should contact the payment networks for updates.

3.9.2 EMV Payment Tokenization

As described in Section 2.7.2, tokens are replacing PANs in mobile phone-based payments and in other payment-enabled devices to enhance the security of the payments ecosystem. Tokens are not used by contactless or dual-interface cards at this time; however, they may be included in the future.

3.9.3 Recommendations

Issuers should consult with the payment networks for guidance on CDCVM and tokenization implementation.

Issuers will need to work with their token service providers and trusted service managers to implement tokenization and comply with guidelines for token provisioning.[23]

[23]For more information on tokenization, see EMVCo, "EMV® Payment Tokenisation Specification – Technical Framework," Version 2, Appendix A, Sept. 8 2017 https://www.emvco.com/emv-technologies/payment-tokenisation/; and Secure Technology Alliance, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," October 2014, http://www.securetechalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/

4 Contactless Considerations for Processors

Many processing platforms or gateways have not yet implemented EMV contactless acceptance support. Most acquirers and acquirer processing entities support contactless, but other entities may not have implemented contactless across all of their platforms or gateways.

Processors who are considering implementing or integrating contactless payment acceptance should therefore consider the following:

- Testing and certification
- Data quality
- Education

4.1 Testing and Certification

Acquiring processors still work with a mix of value-added resellers (VARs) and developers who are focused on implementing MSD rather than EMV contactless. Processors can guide and educate third-party vendors about the value of implementing EMV contactless and provide current payment network testing requirements. In addition, some payment networks do not require EMV contactless implementation, which can be confusing to these partners. There is also a perception that EMV contactless requires double or triple the number of test cases required to certify EMV contact transactions. For more information on testing and certification requirements, refer to each payment network's test requirements and to the U.S. Payments Forum white paper, "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community."[24]

EMV contactless kernel management is different from EMV contact kernel management in that each payment network, rather than EMVCo, manages Level 2 certification. EMVCo is now performing Level 2 certification on new contactless terminals, and these certifications could be used if the payment networks have adopted the EMVCo contactless approval process. Each payment network has its own Level 2 approval process, which affects the terminal vendors' operational approval processes. This difference could translate into different Level 2 LOA expiration dates, which could affect the contactless terminal certification requirements. Processors therefore must plan contactless certification with their downstream partners (VARs, independent sale organizations (ISOs), gateways, and merchants), knowing that contactless kernels expire at different times.

Contactless issuer processors also need to consider the significance of card approval expiration dates, which may be different for the different payment networks and also may depend on what the card vendors have requested as the end-of-life date for a specific contactless product. Issuer processors must manage their card inventory to remove cards after approval has expired. Card inventory management is further complicated for issuer processors by the requirement to work with different card personalization partners, both internal and external.

[24] "EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," U.S. Payments Forum, http://www.uspaymentsforum.org/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/.

Downstream partners (ISOs, VARs, gateways) may not be enabled for contactless, and network connectivity to the acquirer may not be validated before a merchant partner enables contactless. The entire transaction flow must be appropriately tested and certified with the acquirer processor.

4.1.1 Recommendation

EMV contactless testing and certification is well understood by many entities in the payments ecosystem. Processors should contact their testing partners or payment networks for more information.

4.2 Data Quality

In connection with EMV processing, each payment network has specific requirements regarding the data elements and the values of those data elements that need to be present in EMV transactions. For merchants and acquiring processors, it can be challenging to ensure that all data elements are properly populated for the different transaction scenarios that may arise. Issuers rely on the data provided in the EMV transaction to make an educated decision when evaluating transactions for approval.

Issuers and issuer processors use the payment networks' profile certification process to ensure interoperability and compliance with relevant product rules and requirements.

While not a common occurrence, several data quality issues have been identified that create contactless acceptance challenges in the U.S. Terminals supporting MSD contactless transactions may require upgrades to fully comply with the requirements for accepting EMV contactless payments, causing issuers to decline transactions.

For example, merchants with older MSD-only terminals may see the following issues:

- A terminal configured to accept MSD-only contactless is presented with an EMV contactless card, attempts the transaction, excludes the chip data from the transaction, and sends the approval request to the issuer.

  In this scenario, the issuer is expecting EMV data in the message, and the issuer will decline the transaction (for additional information, see Section 2.2.1).

- A contactless interface reads the card data and sends it as MSD swipe transaction.

  CVV/CVC1 failure occurs, as the CVV/CVC is read from the contactless chip and the issuer cannot verify the CVV/CVC.

- Many merchant terminals may incorrectly send POS entry mode 90 - MSD, rather than the contactless entry mode, causing dCVV/dCVC failures.

In addition, the following data quality issues may be seen:

- Transactions may be declining offline for EMV contactless as the EMV capability within the contactless kernel has not been activated properly.
- The issuer or issuer processor may not receive the PAN sequence number (PSN) and not know which card is linked to the specific transaction.
- Issuers may not receive issuer discretionary data and cannot verify the dynamic CVV/dCVC3. This situation can be caused by PCI-related requirements governing track data or end-to-end encryption solutions that may not be encrypting and decrypting track data correctly.

4.2.1 Recommendation

Upgrading to EMV contactless is the most reliable way to ensure that settings are properly established, and that data is of the highest quality, since upgrading requires thorough testing and certification.

Processors should work with merchants and issuers to resolve data quality issues.

4.3 Education

Many resources are available to acquiring processors and their customers to acquaint them with contactless transactions.

Each payment network has a network-specific terminal implementation guide (Table 2) that describes the requirements for terminal deployment in detail. Processors should be familiar with these guides, as well as with the specifications for the processor host/gateway that will be used to connect to the different payment networks. While many aspects of contactless deployments are consistent across multiple networks, other aspects are unique to each network. Contained within each guide are specific requirements, best practices, and similar information.

Table 2. Terminal Implementation Guides

Payment Network	Guide	Version	Date	Additional Resources
American Express	AXP Contactless NFC Terminal Implementation Guide	1.0	Mar 2014	Expresspay Terminal Specification v3.1 Expresspay Terminal Specifications Bulletins
Discover	DPAS US Chip Terminal Guide	1.0	Jan. 2016	Discover Contactless DPAS: Acquirer Implementation Guide v1.2 July 2016 Contactless AIG Discover Contact and Contactless D-PAS: Certification Manual for Issuers and Acquirers v5.0 August 2016 Discover Contact and Contactless D-PAS: Terminal Requirements for U.S. Debit Cards Technical Addendum 2.1 July 2016
Mastercard	M/Chip Requirements for Contact and Contactless	--	Sep. 2017	Mastercard Contactless Terminal Implementation Requirements, April 2017 MC Contactless Kernel Configuration Manual, Feb 2017
Visa	Transaction Acceptance Device Guide (TADG)	3.1	Nov. 2016	Visa Online web site for Visa clients, https://www.visaonline.com Visachip.com Visa Technology Partner web site for vendors, https://technologypartner.visa.com/ Visa clients: Contact your Visa representative. U.S. Terminal whitepaper (Sept 2017) EMV newsletter (monthly)

Payment Network	Guide	Version	Date	Additional Resources
JCB	Discover and PULSE EMV: Terminal Guidelines for JCB Contact and Contactless Chip Cards Acceptance - Technical Addendum	2.0	Oct. 13, 2017	--

In addition to terminal implementation guides, contactless guides or resources may be available from each network. Additional resources include:

- The U.S. Payments Forum (www.uspaymentsforum.org) has compiled a list of resources, including whitepapers, archived webinars, and other educational materials.
- EMVCo has published specifications, specification addenda, white papers, and similar material specific to EMV contactless, mobile, and payment tokenization.
- Third-party entities offer educational and consulting support and testing services. Accredited organizations can assist with EMV contact and contactless migration or implementation. Contact the payment networks to obtain a list of accredited organizations.

5 Conclusions and Recommended Next Steps

The recommendations and best practices included in this white paper address both the perceived and actual challenges of the payment industry in implementing contactless EMV payment – from POS configuration and deployment, processor integration, card issuer consideration and customer experience in the checkout lane. The paper details every step of the key industry stakeholders' contactless deployment journey. By addressing these concerns, the industry can acknowledge contactless as the next generation of payment technology, enabling greater checkout speed for merchants, providing a top of wallet advantage for issuers and creating a smoother deployment for processors.

6 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Payments Council to discuss the challenges of issuing, accepting and processing ISO/IEC 14443/NFC contactless transactions and to help the market work through pre-EMV and post-EMV challenges to promote contactless issuance and acceptance.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members for their contributions. Participants involved in the development and review of this white paper included: American Express; Cardtek; CPI Card Group; Discover Financial Services; Fiserv; G+D Mobile Security; Gemalto; GlobalPlatform; Infineon Technologies; Ingenico; Mastercard; Metropolitan Transportation Authority (MTA); MULTOS International; NXP Semiconductors; Philip Andreae & Associates; TSYS; Visa.

The Secure Technology Alliance thanks **Jack Jania**, Gemalto, and **Oliver Manahan**, Infineon Technologies, who led the project, and the Council members who participated in the project team to write and review the document, including:

- **Andreas Aabye**, Visa
- **Philip Andreae**, Philip Andreae & Associates
- **Charl Botes**, Mastercard
- **Roberto Cardenas**, TSYS
- **Hank Chavers**, GlobalPlatform
- **Jose Correa**, NXP Semiconductors
- **Brady Cullimore**, American Express
- **Jack DeLangavant**, MULTOS International
- **Alan Fong**, American Express
- **Allen Friedman**, Ingenico
- **Melanie Gluck**, Mastercard
- **Murat Guzel**, Cardtek
- **Gokhan Inonu**, Cardtek
- **Jack Jania**, Gemalto
- **Cindy Kohler**, Visa
- **Kenny Lage,** Discover Financial Services
- **Oliver Manahan**, Infineon Technologies
- **Joshua Martiesian**, MTA
- **Cathy Medich**, Secure Technology Alliance
- **Jason Muncey**, American Express
- **Keith North**, CPI Card Group
- **Nick Pisarev**, G+D Mobile Security
- **Jamie Topolski**, Fiserv

Trademark Notice

About the Secure Technology Alliance Payments Council

The Secure Technology Alliance Payments Council focuses on securing payments and payment applications in the U.S. through industry dialogue, commentary on standards and specifications, technical guidance and educational programs, for consumers, merchants, issuers, acquirers, processors, payment networks, government regulators, mobile providers, industry suppliers and other industry stakeholders.

The Council's primary goal is to inform and educate the market about the means of improving the security of the payments infrastructure and enhancing the payments experience. The group brings together payments industry stakeholders to work on projects related to implementing secured payments across all payment channels and payment technologies. The Payments Council's projects include research projects, white papers, industry commentary, case studies, web seminars, workshops and other educational resources.

Additional information on the Payments Council can be found at https://www.securetechalliance.org/activities-councils-payments/.

7 References

"Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers," Secure Technology Alliance Payments Council, June 2016, https://www.securetechalliance.org/publications-contactless-emv-payments-benefits-for-consumers-merchants-and-issuers/

"Contactless Payment Security Q&A," Secure Technology Alliance Payments Council, December 2016, https://www.securetechalliance.org/publications-contactless-payment-security-qa/

EMV Connection web site, http://www.emv-connection.com

"EMV® Payment Tokenisation Specification – Technical Framework," Version 2, EMVCo, Sept. 8, 2017 https://www.emvco.com/emv-technologies/payment-tokenisation/

"EMV Testing and Certification White Paper: Current Global Payment Network Requirements for the U.S. Acquiring Community," U.S. Payments Forum Testing and Certification Working Committee, December, 2017, http://www.uspaymentsforum.org/emv-testing-and-certification-white-paper-current-global-payment-network-requirements-for-the-u-s-acquiring-community/

"Implementation Considerations for Contactless Payment-Enabled Wearables," Secure Technology Alliance Payments Council, October 2017, https://www.securetechalliance.org/publications-implementation-considerations-for-contactless-payment-enabled-wearables/

"An Issuer's Guide to Contactless Payments in the U.S.," Secure Technology Alliance Payments Council, January 2017, https://www.securetechalliance.org/publications-contactless-payments-in-the-u-s-guides-for-merchants-and-issuers/

"Optimizing Transaction Speed at the POS," U.S. Payments Forum Oct. 2017, http://www.emv-connection.com/optimizing-transaction-speed-at-the-point-of-sale/

Secure Technology Alliance web site, http://www.securetechalliance.org

"Technical Solution for Transit Contactless Open Payments Use Case 1: Pay As You Go/Card," U.S. Payments Forum Transit Contactless Open Payments Working Committee, Sept. 2017, http://www.uspaymentsforum.org/technical-solution-for-transit-contactless-open-payments-use-case-1-pay-as-you-gocard/.

"Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," Secure Technology Alliance Payments Council, October 2014, http://www.securetechalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/

U.S. Payments Forum web site, http://www.uspaymentsforum.org

"Understanding the U.S. EMV Fraud Liability Shifts," U.S. Payments Forum, July 2017, http://www.uspaymentsforum.org/understanding-the-u-s-emv-fraud-liability-shifts/.