White Paper

LEVERAGING THE MOBILE CHANNEL FOR ACH PAYMENT INNOVATION

This paper is intended for educational purposes only. It should not be relied upon for legal advice. Readers should consult attorneys for legal advice.

PAYMENTS
INNOVATION
ALLIANCE™
CONNECT. ENGAGE. TRANSFORM.

About "Leveraging the Mobile Channel for ACH Payment Innovation"

The Payments Innovation Alliance, a membership program of NACHA — The Electronic Payments Association, developed this paper. The goals of this paper are to:

1. Support payments innovation via the ACH Network through documentation of the current landscape of ACH mobile payments;
2. Inform the industry of the role mobile technology plays in payments made via the ACH Network.

For the purposes of this paper, a mobile device is defined as a handheld, portable, electronic device used for wireless radio wave communications, such as a cell phone, smartphone, tablet or wearable device. Although some laptops might technically fit within this definition, the authors determined that laptops should remain out of scope.

About the Payments Innovation Alliance

The Payments Innovation Alliance brings together diverse, global stakeholders to support payments innovation, collaboration, and results through discussion, debate, education, networking, and special projects that support the ACH Network and the payments industry worldwide. The Alliance brings together content and focus across all payment areas, including emerging payment technologies, electronic billing and presentment, mobile, payment security/risk, check conversion and global payments. Membership includes organizations of all sizes and spans the payments industry spectrum.

About NACHA – The Electronic Payments Association

Since 1974, NACHA – The Electronic Payments Association has served as trustee of the ACH Network, managing the development, administration and rules for the payment network that universally connects all 12,000 financial institutions in the U.S. The Network, which moves money and information directly from one bank account to another, supports more than 90 percent of the total value of all electronic payments in the U.S. Through its collaborative, self-governing model, education, and inclusive engagement of ACH Network participants, NACHA facilitates the expansion and diversification of electronic payments, supporting Direct Deposit and Direct Payment via ACH transactions, including ACH credit and debit payments, recurring and one-time payments; government, consumer and business transactions; international payments, and payments plus payment-related information. Through NACHA's expertise and leadership, the ACH Network is now one of the largest, safest, and most reliable systems in the world, creating value and enabling innovation for all participants. Visit www.nacha.org for more information.

Acknowledgements

This paper was developed with the collaboration of many stakeholders. The Payments Innovation Alliance would like to acknowledge its members who provided recommendations and expertise during its creation.

Edward Bachelder,
Director, Research,
Blueflame Consulting LLC

Douglas Bondick, AAP,
Product Manager,
Wells Fargo

Marcela Cauthon, AAP,
NCP, Product &
Services Manager,
EPCOR

Edward M. Craig,
President,
Electrum Corporation

Susan K. Doyle, AAP,
Vice President,
Commerce Bank

Stephen K. Kenneally, AAP,
Vice President, Center
for Payments and
Cybersecurity Policy,
American Bankers
Association

Mohammad Khan,
Board Director,
OmnyPay

Reed Luhtanen,
Senior Director,
Payments Strategy,
Wal-Mart Stores Inc.

Phyllis C. Meyerson, AAP,
CCM, Executive Vice
President,
ECCHO

Michael Mulholand,
Director, Fraud Solutions,
FIS

Anita S. Patterson, CTP,
Director,
Treasury Services,
Cox Enterprises Inc.

Lawrence W. Proctor, AAP,
Operational Risk
Consultant,
Wells Fargo

Kathleen Rakers,
Product Manager,
U.S. Bank

Orlando Santos,
Vice President,
Treasury & Payment
Solutions,
Webster Bank

William J. Schoch,
President and CEO,
Western Payments
Alliance

Kerry Sellen, AAP,
Vice President,
Compliance,
TeleCheck Services Inc.

Brad Smith, AAP,
Senior Manager,
Enterprise Payments,
Capital One

Les Smith,
ACH Sales and
Business Development,
Jack Henry & Associates

Charla Tompkins, AAP,
Supervisor - Savings &
Checking, Programs
and Analysis,
Navy Federal Credit Union

Uma Wilson, AAP, CTP,
Senior Vice President &
Director, Product
Management &
Development,
UMB Bank, NA

Note: The views presented in this white paper do not necessarily reflect the individual views of each member of the project team, the entities or organizations that employ the members of the project team, the Payments Innovation Alliance Leadership Team, or the individual Alliance member organizations.

Executive Summary

Current Landscape

Mobile payments, which remain in a state of innovation, have been a key topic for the payments industry for several years. However, with the introduction of new mobile point-of-sale (POS) payment solutions by major players in the industry, the increasing utilization of mobile devices by both consumers and corporates, and the continued growth and evolution of the ACH Network to meet industry needs, the industry and mobile payments stand at an important crossroad.

There are many methods of initiating and receiving mobile payments, but this paper will focus on the use of mobile devices with ACH transactions, rather than all mobile payments.

How to Utilize the Mobile Channel for ACH

Mobile devices are used currently for both remote and proximity payments made via the ACH Network.

Bill Pay – Biller Direct	Bill Pay – Online Banking	P2P – Online Banking	P2P –Non-FI
Check Conversion	Proximity Payment at the POS	Internet spontaneous purchases	Corporate – payroll and vendor payments

It is important to note that all of the same regulations and rules that apply to an ACH payment must be followed, and all of the required disclosures and notices must be provided, and all data protected, regardless of whether or not a mobile device is utilized in an ACH payment. Despite the fact that many mobile devices utilize small screen sizes, products and services delivered on mobile devices must still provide a fully compliant experience to users.

The NACHA Operating Rules and Guidelines (Rules) provide the legal foundation for the ACH Network and are used by the financial services industry to receive, process and/or originate ACH credit and debit payments, including those that utilize a mobile device. This paper contains a framework for determining the appropriate Standard Entry Class (SEC) Code to employ when utilizing a mobile device in compliance with the *Rules*.

Benefits and Opportunities

There are many opportunities to incorporate a mobile device into an ACH transaction and multiple benefits for all participants -- merchants, billers, consumers, corporate treasury professionals, financial institutions and third parties -- including:

- the ability to make/approve and receive ACH payments wherever and whenever desired in an easy, quick and convenient fashion;

- the ability to reduce costs by replacing check and card payments with lower cost ACH payments;
- the creation of additional customer payment methods;
- the ability to enhance the payment experience through analytical services and loyalty programs;
- the opportunity for smaller businesses to utilize electronic payments;
- the enhanced authentication methods provided by the mobile device;
- the enhanced security provided by the mobile device;
- the access to ACH payments provided by the mobile device for the underbanked; and
- the ability to strengthen relationships with corporate customers by offering desired services.

Risks and Challenges

There are certain risks applicable to any type of ACH payment, and these "traditional" ACH payment risks still apply to ACH payments with or without the utilization of a mobile device. There also are some additional risks unique to the mobile channel, including security risks stemming from the user or the payment application, technological risks consisting of battery/coverage issues, device size, and the rapid pace of technological change in the mobile space, as well as product risks, including adoption, compliance and poor customer experience. As with any ACH transaction, when adding mobile to an ACH payment, the type and level of risk associated with the transaction should be considered. This paper discusses a variety of risk mitigation techniques available, including the additional authentication methods made possible by the use of a mobile device.

Conclusion

Consumers and businesses are using mobile devices to make payments, and having an overarching mobile strategy is now a key component of an organization's success. Leveraging the mobile channel for ACH payments offers opportunities for merchants, billers, consumers, corporate treasury professionals, financial institutions and third parties.

Mobile devices are being incorporated into ACH transactions already, and while their current use is fairly limited, corporate ACH payments utilizing a mobile device are beginning to gain traction. ACH is being utilized successfully in some POS mobile applications, particularly in the convenience/fuel retail industry, and ACH is well-suited to, and commonly used with, mobile bill pay, mobile P2P and m-commerce solutions.

With the convergence of consumer and corporate adoption of mobile devices, the new awareness of mobile payments sparked by the introduction of new near field communication-based POS mobile solutions, and the continued evolution and growth of the ACH Network to meet industry needs, it appears the use of mobile devices in ACH transactions is poised to grow dramatically in the next three years.

Current Landscape

In the short time since the introduction of Apple and Android smartphones, mobile payments have become a reality. Although mobile payments remain in a state of innovation, and experts continue to speculate on their future, both established and new companies are entering the market as early adopters. The full impact of mobile on the payments industry is yet to be seen; however, new considerations are emerging for industry stakeholders as the ACH Network increasingly is utilized for these types of payments.

In 2009-2010, the NACHA Internet Council focused on payments made via this channel and helped to lead NACHA rulemaking efforts for payment functionalityand security. In 2010, the Mobile ACH Payments Rule was approved with an effective date of January 1, 2011. The Rule incorporated mobile ACH debits into the pre-existing category of Internet-Initiated Entries (WEB) by requiring that ACH payments authorized and/or initiated via wireless networks use the WEB Standard Entry Class (SEC) Code. Mobile devices also can be used when originating other SEC codes such as BOC, CIE, CCD, POP, POS and PPD.

While there are many methods of initiating and receiving mobile payments, this paper will focus on the use of mobile devices with ACH transactions, rather than all mobile payments. Mobile devices are used currently for both remote and proximity payments made via the ACH Network for bill payments, payments at the point of sale, person-to-person (P2P) payments, Internet purchases, and corporate payments (both payroll initiation and trading partner payments).

With the introduction of new mobile POS payment solutions by major players in the industry, the increasing utilization of mobile devices by both consumers and corporates, and the continued growth and evolution of the ACH Network to meet industry needs, the industry and mobile payments stand at an important crossroad.

Current Use of Mobile Payments

In less than 10 years, mobile use, and in turn, mobile payments, has grown to an increasingly expected and used platform for millions of consumers and businesses. As adoption of mobile devices has increased, so too has the expectation that the phone will offer payment solutions – for bill payment, at the point of sale, for P2P payments, and beyond. Study after study finds the growth in mobile payments as a driving force for industry change.

2007 and 2008 introduced the first iPhone and the Android phone respectively. Since then, products such as Square have popularized mobile card acceptance and new payment technologies are being utilized, such as Quick Response (QR) codes, Near Field Communication (NFC), Host Card Emulation (HCE), and Bluetooth Low Energy (BLE). There are a variety of mobile and digital wallets available, and numerous mobile applications that involve payments in some way.

According to the March 2014 Federal Reserve Board report, *Consumers and Mobile Financial Services*, 87 percent of U.S. adults have a mobile phone and 61 percent of mobile phones are smartphones, meaning they are Internet-enabled. Seventeen percent of all mobile phone owners and 24 percent of smartphone users have made a mobile payment in the last 12 months, most commonly a bill payment. Additionally, 17 percent of smartphone users have used a mobile device to make a payment at the point of sale. According to a Javelin Strategy and Research report released in October 2014, *Mobile Wallets Analysis and Strategy*, the percentage of consumers purchasing physical goods over mobile phones has more than tripled since 2009.

With this broad adoption, mobile is becoming an increasingly important channel for billers. According to a survey by Blueflame Consulting of 128 billers, on average, almost one in five visits to an organization's website occur on a mobile device, and the top activity at the site is bill payment. Fiserv's 2014 *Seventh Annual Billing Survey* showed that from 2011 to 2014, the percentage of mobile bill payers grew by 69 percent. The 2013 *Federal Reserve Board Payments Study* showed that there were 2.5 billion online and mobile bill payments initiated, with 93 percent initiated through a Web browser (online and mobile combined) and the remaining 7 percent initiated through an application or SMS/text message. As the ability to pay a bill with a mobile device becomes a consumer expectation, biller deployments will likely increase.

Mobile is used at the point of sale and for P2P payments as well. The Federal Reserve Board study showed that more than 250.6 million mobile payments were made using a mobile wallet application in 2012. There were also 205.3 million P2P payments made, of which 68 percent were browser-initiated (online and mobile combined), 32 percent were initiated using a mobile application, and less than 1 percent were initiated via SMS/text message. According to the Javelin report, consumer mobile purchases made via a mobile browser and application far exceeded mobile purchases made at the point of sale.

It should be noted that the above statistics include all payments made via a mobile device, regardless of the payment rails used (card or ACH).

Mobile Remote and Proximity Payments

There are two types of mobile payments: remote and proximity payments. Each type serves different user needs and use cases and offers opportunities for broader mobile payments adoption.

Remote mobile payments can be facilitated in several ways. These payments can be browser-based, meaning they are processed in the same manner as an online payment, but a mobile device is used rather than a laptop or desktop computer. Mobile payments also can be initiated via a downloaded application (app), meaning an app on the device is accessed to make the payment. Remote mobile payments also can utilize SMS/text, in which text messages are sent to initiate the payment. Examples of remote payments include P2P payments, bill payments, and making purchases online via an application or mobile website.

Mobile devices also can be used for proximity payments at the point of sale, using technologies such as near field communication (NFC), Host Card Emulation (HCE), Bluetooth Low Energy (BLE), and quick response (QR) code.

NFC permits two devices that are equipped with an NFC chip to exchange data when placed close together. Once the connection is made, the user is often asked to authenticate via biometrics (such as a fingerprint, voice recognition, etc.) or password/code. There is a secure element either in the mobile device itself, or located in the cloud if HCE is used, which stores the payment credentials (card or bank account information), and communicates the information to the other device. The use of HCE requires connectivity for the solution to work, and mobile data coverage is still not consistently reliable in retail locations across the United States. The recently introduced Apple Pay is an example of a solution utilizing NFC technology.

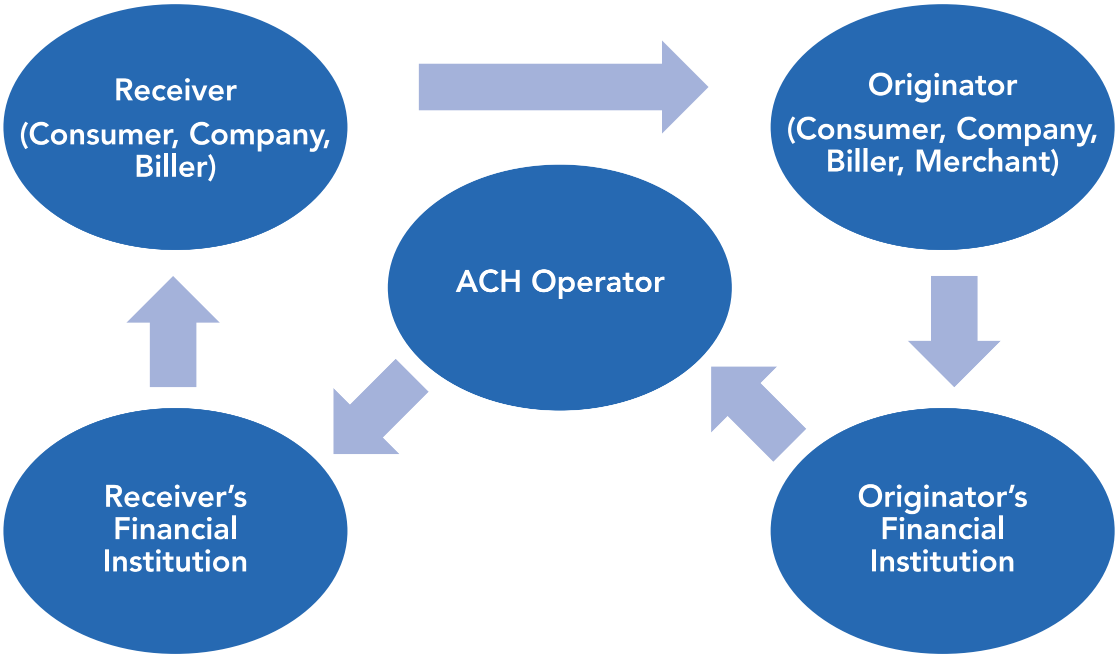
BLE technology can be a substitute for, or a complement to, NFC. Like NFC, it is a wireless method to transmit data short distances. NFC requires very close proximity to work, and both BLE and NFC require new POS acceptance technology. In addition to payments, BLE also can be used for analytical services and loyalty programs, as it is able to detect users' phones when entering retail locations. PayPal's Beacon is an example of a solution utilizing BLE technology.

A QR code is a two dimensional bar code that, when used at the point of sale, provides information for the payment transaction. Merchants can scan a QR code created by an application on the customer's mobile device that contains payment credentials, or the customer can scan the QR code created by the merchant's system with payment details, and then pay within the mobile application. Merchant Customer Exchange (MCX), a coalition of large merchants, plans to implement CurrentC, a QR code payments solution, in 2015.

Role of Mobile in ACH Transactions

Today, many ACH payments utilize a mobile device along with the traditional ACH payment flow. As of Q4 2014, year-over-year growth of WEB payments was nearly 13 percent, making these payment types responsible for one-fifth of total Network volume. This growth is attributable in part to the rise in mobile ACH payments.

The flexibility and versatility of the ACH Network allow for mobile payments to be both debit payments (when an individual or business authorizes a pull of money from the account) and credit payments (when a person or business authorizes a push of funds from the account). This attribute offers new opportunities for both senders and receivers of mobile payments.


Receiver
(Consumer, Company, Biller)
Originator
(Consumer, Company, Biller, Merchant)
ACH Operator
Receiver's Financial Institution
Originator's Financial Institution

A typical ACH transaction has an originating company or individual (Originator); an Originating Depository Financial Institution (ODFI), which is the Originator's financial institution; an ACH Operator; a Receiving Depository Financial Institution (RDFI), which is the Receiver's financial institution; and a receiving company or individual (Receiver). Sometimes a Third Party Service Provider also is used by one or more of the participants.

Consumers are Originators when they use mobile devices to access their financial institution's website and authorize bill payments or P2P payments. Businesses use mobile devices to originate transactions to pay their employees or to pay vendors. Merchants accept checks and use mobile devices to obtain the information to convert the check to an electronic payment via ACH or to originate a debit for bill payment or at the POS.

Consumers and businesses are Receivers when they utilize a mobile device to authorize a debit to their bank account at a biller's website, or on the Internet to pay for a purchase or to pay a trading partner. They also act as Receivers at the point of sale when they use a mobile device to allow a debit to a bank account that they have linked to the device. (See Appendix for detailed descriptions of various scenarios of ACH transactions utilizing mobile devices.)

How to Utilize the Mobile Channel for ACH Transactions

It is important to note that all of the same regulations and rules that apply to an ACH payment must be followed, and all of the same disclosures and notices provided, and all data protected, regardless of if a mobile device is utilized in an ACH payment. The primary source for rules and regulations for the commercial ACH Network is the *NACHA Operating Rules. Title 31 Code of Federal Regulations Part 210* governs federal government payments. Other applicable laws for ACH transactions include the *Uniform Commercial Code Article 4 and 4A* and the *Electronic Funds Transfer Act* as implemented by *Regulation E. The Right to Financial Privacy Act, the Electronic Signatures in Global and National Commerce Act, Regulation D, Regulation CC* and other regulatory agency directives also can impact ACH payments. Like all payments methods, the ACH Network is required to comply with Office of Foreign Assets Control-enforced sanctions policies. All U.S. ACH participants should be aware that they can be held accountable and should understand their compliance obligations.

Despite the fact that many mobile devices utilize small screen sizes, products and services delivered on mobile devices must still provide a fully compliant experience to customers and consumers, including:

- appropriate disclaimers/disclosures delivered as required;
- the ability to read and understand terms and conditions;
- the ability to make clear choices and understand fees and charges as required; and
- the ability to retain copies of terms, receipts, etc., as applicable.

Similarly, the use of a mobile device does not relieve those offering mobile products and applications from compliance with the *Americans with Disabilities Act* and Network participants should be aware that some devices work better than others in terms of complying with the requirements.[1]

[1] Recent court cases such as National Federation of the Blind v. H&R Block (http://www.ada.gov/hrb-cd.htm) require businesses using mobile devices for commerce to meet W3C WCAG 2.0 (Worldwide Web Consortium Web Content Accessibility Guidelines 2.0) Level AA success criteria http://www.w3.org/TR/WCAG20/.

Appropriate Standard Entry Class (SEC) Code Use When Utilizing a Mobile Device

Rules to support ACH mobile payments were created in January 2011 to provide a framework for the financial services industry to receive, process and/or originate mobile-initiated ACH consumer debit payments. The rules for mobile payments were incorporated into the existing rules and requirements for Internet-initiated consumer debit entries, which are classified in the ACH Network using the WEB SEC Code. Other SEC codes are sometimes applicable as well when a mobile device is utilized in an ACH transaction.

Scenarios Where Mobile Devices Are Used in ACH Transactions	SEC Code to Use
The Receiver uses a mobile device to authorize a debit entry over a wireless network, or the Receiver uses a mobile device to initiate a debit entry over a wireless network even if the authorization was given in another manner.	WEB
Consumer initiates or authorizes a consumer to consumer credit entry such as P2P via a mobile device.	WEB
A consumer uses a mobile device in person at the Originator's (merchant's) electronic terminal to initiate debit entry to their bank account to pay for goods or services, or to receive cash back. Electronic terminals include traditional POS terminals such as store cash registers or automated fuel pumps, as well as mobile devices used as mobile checkout terminals.	POS (WEB is not appropriate if POS would otherwise apply because the WEB format does not include all of the necessary fields to communicate the POS transaction information.)
A consumer initiates a credit entry to a non-consumer (business) account via a mobile device. These entries are usually transmitted through an online or mobile banking product or bill payment service provider website or mobile site.	CIE
An Originator uses a mobile device to capture Magnetic Ink Character Recognition (MICR) line information from a check at the point of purchase or later for subsequent conversion during back-office processing and the check is not returned to the Receiver.	BOC
An Originator uses a mobile device to capture MICR line information from a check at the point of purchase and the check is returned to the Receiver.	POP
A business uses a mobile device to initiate transactions to pay trading partners.	CCD
A business uses a mobile device to issue payroll to its employees.	PPD

Additional Rules and Regulations when Utilizing a Mobile Device

Although all of the rules and regulations that would ordinarily apply to an ACH transaction still apply when utilizing a mobile device, there may be additional requirements as well. For example, if SMS/text messages are used as part of a mobile product, businesses should be aware that they must comply with the *Telephone Consumer Protection Act*, which requires prior express consent before sending SMS/ text messages. In addition, there may be federal and state privacy laws (including *Children's Online Privacy Protection Act*) that apply.

Benefits and Opportunities

The ACH Network offers cost-effective, efficient payment solutions for mobile device users, with a low incidence of fraud when properly instituted. In fact, ACH credits are one of the safest payment types.[2] Leveraging the mobile channel for ACH payments offers opportunities for merchants, consumers, corporate treasury professionals, financial institutions and third parties.

Merchants

A merchant is the originator of POS proximity purchases, online purchases done with a mobile device, and mobile check conversion transactions. Many merchants see mobile payments as an efficient way to utilize ACH for cost-savings. Enabling the use of mobile devices for POS transactions allows a merchant to leverage a low-cost ACH payment, while simultaneously taking advantage of abilities to cross-sell, incorporate loyalty and rewards programs with the mobile payment, and to provide coupons to their current and future customers. In addition, the portability of the device ensures that both the merchant and customer have the ability to make and receive payments wherever and whenever they want to do so, in an easy, quick and convenient fashion.

ACH and mobile can work together to create additional customer payment options and provide an alternative to check and card payments. Enrolling customers in an ACH program for online or POS payments in advance can reduce the merchant's risk, as there is additional time to authenticate and verify payment credentials prior to the transaction. Some smaller merchants find card acceptance cost prohibitive and overly complicated, but might be able to leverage the mobile channel and ACH to adopt a low-cost form of electronic payments.

Billers

Billers also see benefits from utilizing mobile with ACH transactions. Just as with merchants, mobile allows their customers to pay bills wherever and whenever they desire given the portability of the device. The use of a QR code allows the customer to scan a bar code located on the bill with their mobile device to obtain the necessary information to make the payment.

Users who like to pay their bills via a mobile device do so because it is easy, efficient, available regardless of location or time, and allows them to pay at the last minute if needed. Mobile payment has become an expected option for most consumers, and billers are seizing the opportunity to provide enhanced customer service while reducing costs and encouraging paperless billing.

Both billers and merchants enjoy the enhanced authentication abilities provided by the use of a mobile device in an ACH payment, as it allows an Originator to more easily verify users are who they claim to be when making the payment.

[2] See the *2014 AFP Payments Fraud and Control Survey* found at http://www.afponline.org/fraud/

Consumers

Consumers are both originators and receivers of credits in P2P payments, originators of credits in online banking bill pay, and the receiver of debits in biller direct bill pay, POS proximity payments and check conversion. Just as with billers and merchants, consumers like having the ability to make payments wherever and whenever they choose, in a convenient, easy way, without having to carry cash, checks, or cards with them. Using a mobile device to make an ACH payment can help a consumer avoid late fees, and can provide enhanced security as both the phone and the application can be protected via a password and/or biometric solution. Studies have shown that many consumers do not like incurring debt and would prefer a payment method that directly deducts the payment from their financial institution account.

Underbanked or unbanked consumers can benefit from mobile devices utilizing ACH payments as well. Mobile devices can provide access (seen often with prepaid card "accounts") to ACH payments such as Direct Deposit, billpay, Internet purchases, and P2P services.

Corporate Treasury

Although most corporate banking is still performed on traditional desktop or laptop computers, increasingly companies whose treasury departments serve as the originator for payroll or vendor payments are using mobile devices to authorize and initiate ACH credit transactions. Corporate transactions often require multiple individuals' approval, and when one individual is out of the office, the entire process can be delayed. Incorporating the use of mobile into their ACH approval/initiation process can allow corporate treasury staff to remain productive even when out of the office or in a meeting. It provides an easy, convenient way to increase office efficiency, and serves as another way to make payments when used as part of business continuity/disaster recovery plans.

Financial Institutions and Third Parties

Adding mobile as a channel for ACH gives financial institutions and third parties the ability to provide their customers with the services they want and need, which strengthens their relationship with existing customers and helps to attract new customers from organizations that do not offer these services. Mobile creates a new channel for a customer to use for ACH transactions and provides enhanced security and authentication techniques.

Risks and Challenges

All payment types require appropriate risk-mitigation techniques to ensure the safety, security and integrity of the payment. Utilizing a mobile device to make an ACH payment offers significant opportunities that must be supported by thorough risk assessments and proper protocols.

For any ACH payment, users should consider credit risk, operational risk, fraud risk, systemic risk and reputational risk. When leveraging the mobile channel, there are a few additional channel-specific considerations that apply to any type of mobile payment: security and data protection, technological challenges and payment product considerations.

Security / Data Protection

Mobile device users are the first line of defense in properly securing mobile ACH transactions. By following proper protocols – including vigilance around storing and locking down the device, updating operating systems and apps, and being aware of phishing scams – a user can greatly diminish risks associated with mobile payments. Educating users to be mindful of what's on their devices and how to protect that information helps to reduce mobile payment risk.

A mobile device, by definition, is portable, so there is the risk of the device being lost or stolen or simply left unattended in a public setting, but the risk can be reduced if the user takes steps to safeguard the device. For example, if the user protects the device with a passcode or other means, the information stored on the device is less likely to be accessible and/or the applications on the device utilized by someone other than its owner.

Updates for mobile device operating systems and apps often are meant to patch security issues. When users are proactive in downloading updates, it raises the likelihood of all versions of an app or system having the same level of security. Users also should be educated to take appropriate care when downloading applications to the device, as malware and viruses can be hidden in applications that appear to be legitimate. Users should be encouraged to run anti-malware or virus protection software on their mobile device, just as they do on their laptop/desktop computer, to minimize the chances of an infected device being used to make a payment. In addition, users should be warned to be cautious about utilizing public, unsecured Wi-Fi with their mobile device, to ensure that their data transmission is secure. And finally, with the addition of a mobile device, the user should be made aware of SMShing (phishing via SMS/text instead of traditional email phishing), and encouraged to exercise appropriate caution when responding to possible phishing text messages. Compounding these potential user risks is the fact that for many mobile applications/sites, the focus is on ease of use, rather than on security, and it can be a challenge to convince a user to utilize what may be viewed as cumbersome security procedures.

The payment application itself poses another risk for payments made utilizing a mobile device. It is critical that security and data protection are a priority for the application developer, as poorly designed applications may not store or transmit data safely. It also is important for the developer to keep in mind the different levels of risk that accompany different types of payments. There are differences between an application designed for a corporate user to initiate payroll or pay a trading partner, and an application designed for a consumer to make routine bill payments, and one designed for purchases at the point of sale.

Technology

There are certain technological risks and challenges that accompany the use of a mobile device. A mobile device poses certain inherent technological risks such as insufficient battery level or a coverage drop that could (along with a broken or not present device) make it impossible to complete a transaction. In addition, the many types of mobile devices available can create challenges for the developer when creating applications. Because of the many available device options for users, it is necessary to program for different platforms (Android, iOS, Windows OS, etc.), as well as to create payment methods that will work for smartphones, tablets, wearables and feature phones.

The small size of a mobile device can create issues as well when attempting to use it for an ACH transaction. It can be difficult to provide information to the user such as required disclosures/notices in a readable format and difficult for the user to input necessary information into the device. In addition, the limitations created by the size of the device tend to create more reliance on the Cloud, which comes with its own risks.

Finally, the fact that mobile technology is evolving and changing so quickly also poses some risks. It is unclear if there will be a single preferred method of mobile payments or if many competing technologies and methods will coexist. A payments provider must balance the risk of moving too quickly and picking a solution that does not last with the risk of moving too slowly and missing an important opportunity.

Product

When creating a mobile payment product, there is the risk that the product, while good, does not solve a problem and/or is not used by the intended audience. There is an additional risk that even if companies and consumers want to use the product, without biller/merchant adoption they will not be able to do so.

There is also some additional compliance risk when utilizing a mobile device. Due to the small size of the device, it can be difficult to ensure the product complies with all existing regulations. Additionally, it is challenging to attempt to anticipate and comply with unknown potential changes to the current regulatory environment. (Please see the section on *How to Utilize the Mobile Channel for ACH Transactions* found earlier in this paper for the complete discussion of compliance requirements.)

There is also the risk of a poor customer experience with a mobile payment product. The additional parties involved when a mobile device is utilized may make it more difficult for users to understand who is responsible when something goes wrong with a payment. A user may have difficulty enrolling in a mobile payment service if they do not know their routing transit number and/or account number. And if a user's device is wiped or destroyed, the user might have trouble restoring all of the information stored on the phone and in the applications. A customer may also have a bad experience if there is not a mobile enhanced site to use. Difficulty with using a mobile device on a site optimized for a laptop/desktop may make it difficult or impossible to complete a payment.

Risk Mitigation

As with any ACH transaction, the Originator should use the type and level of risk associated with a transaction when deciding what risk mitigation techniques are necessary. It is important not to rely on any single control when mitigating risk, but rather to utilize a layered approach to security as suggested by the Federal Financial Institutions Examination Council's (FFIEC's) 2011 *Supplement to Authentication in an Internet Banking Environment*, to aid against the devices being vulnerable to fraud.

The mobile device, as well as any applications related to payments, should require authentication prior to use. Users can leverage the capabilities of mobile technologies to utilize layers of authentication to help lower an Originator's risk. In addition to a password or passcode, biometrics, such as the fingerprint scan utilized by Apple Pay, can be used. Geolocation can be used to determine if the mobile device is in a place consistent with the payment being made. In addition, device verification can be used to identify if the mobile device has been previously registered as belonging to the user making the payment.

Mobile applications should store and transmit data safely, as data must be protected both at rest and in transit. Whenever possible, sensitive data should not be stored on the device itself, and the user should have the ability to wipe the device if lost or stolen.

Education

Through ongoing education and clear instructions, developers and Originators can help ensure proper protocols around mobile payments. Key considerations include:

- Education on keeping the device secure should be provided to users to encourage the use of anti-malware/virus detection software, as well as warnings on the use of public Wi-Fi and downloading of applications from unknown sources, and training on avoiding SMShing.
- Developers and/or Originators may need to provide education to users to ensure they understand how to use the application/mobile site to initiate an ACH payment.
- Developers and/or Originators should provide clear information on who should be called for different issues with the payment solution.

Mobile Device

Mobile devices can be very different with varying sizes, form factors, and operating systems. Developers and Originators should consider the following suggestions to help mitigate the inherent challenges presented by the utilization of a mobile device.

- To aid with accurate data entry on a small screen, Originators may wish to require the double keying of important information with automated verification to ensure the entries match.
- Originators may want to consider providing required information to users in multiple ways, such as via email in addition to providing on mobile device, to ensure they receive and can read required disclosures, receipts, etc.
- Developers should be aware of the different issues that arise with different sized devices, i.e. tablets are different from phones, which are different from wearables, and ensure that applications work regardless of device form.
- It is important for application developers to stay current on updates made to various operating systems to ensure their application continues to work properly, and to ensure that when security related changes are made, users are required to download and use the most current version of the application.

Product Viability

Key considerations for product viability include:

- As with any product, developers may wish to research and conduct focus groups to ensure the product is needed. Because the user is required to change behavior to utilize a mobile device in the initiation of an ACH transaction, incentives may need to be created to drive adoption and change the users' behavior.
- Developers should ensure the technology fits to the market for which it is designed and that the technology utilized can be supported by both Originators and Receivers.

Conclusion

Mobile payments are now an industry reality, and mobile devices are being incorporated into ACH transactions. While their current use is fairly limited, the ACH Network has and will continue to play a role in the movement of funds and payment information via the mobile channel. There is the potential for dramatic growth as utilizing the mobile channel for ACH payments creates a ubiquitous low-cost means of accessing payments.

Consumers and businesses are using mobile devices to make payments, and having an overarching mobile strategy is now a key component of an organization's success. Both new and established companies are entering the market as early adopters and the ACH Network is increasingly utilized for these types of payments.

Although many mobile payment providers continue to focus on consumer payments, there are other emerging opportunities. For example, corporate ACH payments utilizing a mobile device are small in number, but beginning to gain traction with the introduction of corporate mobile applications by several major financial institutions and the growing demand for support of tablet devices. Despite some potential drawbacks to solutions that leverage the ACH Network at the POS, such as 60-day return time frames and the lack of guaranteed funds, ACH is being utilized successfully in some POS mobile applications, particularly in the convenience/fuel retail industry. Finally, ACH is very well-suited to, and commonly used with, mobile bill pay, mobile P2P and m-commerce solutions.

The mobile channel is an extension of the online channel and will likely become an equally or more popular method of makingpayments. Financial institutions, developers, companies and merchants have an opportunity to leverage their relationships with other industry stakeholders to create a valuable role for themselves in this rapidly evolving environment. Those who choose to wait to prepare for the mobile future may pay a high cost for the missed opportunity.

The ACH Network plays an important role in supporting mobile payment innovation. While both established and new mobile payment providers will need to continue to address user security, data protection, evolving technology and other associated risks, utilizing mobile devices in ACH payments is here to stay. With the convergence of consumer and corporate adoption of mobile devices, the new awareness of mobile payments sparked by the introduction of new near field communication-based POS mobile solutions, and the continued evolution and growth of the ACH Network to meet industry needs, it appears the use of mobile devices in ACH transactions is poised to grow dramatically in the next three years.

Additional Resources:

"The Future of Corporate Payments," Payments Innovation Alliance White Paper
https://alliance.nacha.org/system/files/Alliance%20Corporate%20Payments%20White%20Paper%20FINAL.pdf#overlay-context=content/member-resources

"Risk Management Strategy Executive Summary," NACHA
https://www.nacha.org/system/files/resources/Risk%20Management%20Strategy%20Executive%20Summary%281%29_0.pdf

Consumers and Mobile Financial Services, March 2014 Federal Reserve Board report
http://www.federalreserve.gov/econresdata/mobile-devices/files/consumers-and-mobile-financial-services-report-201403.pdf

2013 *Federal Reserve Board Payments Study*
https://www.frbservices.org/communications/payment_system_research.html

Payments Innovation Alliance:
https://alliance.nacha.org/

Regional Payments Associations:
https://www.nacha.org/members/regional-payments-associations

ElectronicPayments.org:
www.ElectronicPayments.org

Risk Updates and Resources:
https://www.nacha.org/risk

Training Resources:
https://www.nacha.org/events/training-resources

Appendix: Current ACH Use in the Mobile Environment

This table lists scenarios for using a mobile device in an ACH transaction, and does not include mobile transactions that use debit, credit or prepaid cards. In many cases, a prepaid or stored value account, which the user opts to fund via ACH, could be used in place of an ACH entry for the specific transaction; however, these are not detailed below as the actual interaction of mobile device and payment is not utilizing ACH. The examples of companies offering these services are not an all-inclusive list, but merely a sample. The table does not contain all of the required *Rules* obligations for the various transactions. For a complete discussion of applicable Rules for each entry type, please see the *NACHA Operating Rules*.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Bill Pay (Biller Direct) with mobile device authorization	Examples include utilities such as Georgia Power and telecoms such Verizon and AT&T	A consumer uses a mobile device to access a billing company via a mobile web browser or downloaded application. The consumer authorizes a debit to his checking account to pay a bill. The biller originates a WEB debit to the consumer's account.	The use of a mobile device does not change the authentication and authorization requirements for the biller. However different methods may be used for authentication that take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the biller's account at its financial institution will be credited. Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The biller's company name will appear on the consumer's bank statement.
Bill Pay (Biller Direct) with mobile device initiation	Examples include utilities such as Piedmont Natural Gas, Virginia Beach Public Utilities and Carroll Electric	A consumer authorizes a bill payment (in person, via the Internet, on the phone) but confirms/initiates the payment by utilizing a mobile device, based upon a preference designated during the enrollment process. The consumer receives a text message or application push notification that a bill is available or due, with instructions on how to reply to initiate a payment. Regardless of the manner or channel by which the consumer enrolled, authorized, and provided account information for the payment, the billing company originates a WEB debit to the consumer's account to pay the bill because the billing company has designed a payment initiation procedure using a wireless network.	The use of a mobile device doesn't change the authorization and authentication requirements; however, the authorization and part of the authentication process takes place during enrollment when the consumer authorizes the payments, not during the confirmation/ initiation process. The biller should employ the same level of authentication as it would for online initiation, but additional and /or different methods may be used for authentication, which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the biller's account at its financial institution will be credited. Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The biller's company name will appear on the consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Online Banking Bill Pay with mobile device	Financial Institutions (large and small)	A consumer uses a mobile device to access his/her financial institution's website via a mobile web browser or downloaded application. The consumer sets up a bill payment to be made, or confirms a previously arranged or recurring bill payment. The financial institution initiates a CIE credit to the biller's account at the RDFI.	The use of a mobile device does not change the authentication requirements and the financial institution should employ the same levels of authentication as it would for originating non-mobile CIE credits via online banking. Additional and/or different methods may be used for authentication, which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the biller's account at its financial institution will be credited. (The financial institution may choose to use a good funds model, in which the debit to the consumer's account occurs before the credit is sent as a risk management tool.) Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The biller's company name will appear on the consumer's bank statement.
Online Banking Bill Pay with mobile device using Third Party Service Provider	Examples of Third Party Bill Payment Service Providers for financial institutions include: ACI, FIS, Fiserv, and iPay.	In this variation, the financial institution does not host the bill payment application itself, but instead contracts with a third party for the bill payment service. When a consumer uses a mobile device to access his/her financial institution's website via a mobile web browser or downloaded application, the consumer is "handed off" to the website / application of the third party. The consumer sets up a bill payment to be made, or confirms a previously arranged or recurring bill payment. The third party effects the complete transfer of funds from the consumer's account to the biller's account using the split transaction model with two discrete ACH transactions: 1) a WEB debit to the consumer's account to collect the funds for the bill payment, and 2) a CIE credit to send the funds to the biller.	The use of a mobile device does not change the authentication requirements and the Third Party Service Provider should employ the same levelsof authentication as it would for originating non-mobile CIE credits and WEB debits. Additional and/or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the biller's account at its financial institution will be credited. (The third party may choose to use a good funds model, in which the debit must clear (e.g., is not returned NSF) before the credit is sent, as a risk management tool.) Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The biller's company name will appear on the consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Mobile Proximity Payment at the Point of Sale – QR Code	Used at retail locations. Examples of merchants include MCX (a large merchant coalition), and service providers include Paydient	A consumer is ready to checkout at a merchant. The consumer uses his/her mobile device to open the downloaded application for that merchant at the point of sale (POS). The application generates a bar code that is read by the retailer's scanner to complete the transaction based on the bank account information that was provided by the consumer during the initial enrollment process. The merchant originates an ACH debit to the consumer's account using the POS SEC code In a variation of this scenario, when the customer is ready to check out at the POS, the merchant generates a bar code with billing details that is read by the consumer's phone. The customer initiates a payment from within the mobile application and the merchant originates an ACH debit to the consumer's account using the POS SEC code.	The consumer is confirming/initiating the payment utilizing their mobile device based upon information/authorization provided during the enrollment process. The consumer may be prompted for authentication such as a PIN or password and additional and/or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the merchant's account at its financial institution will be credited. Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The merchant's company name will appear on the consumer's bank statement.
Mobile Proximity Payment at the Point of Sale – NFC	Could be used at any retail location utilizing NFC. Most current NFC solutions use credit or debit cards as payment methods, but there is no reason ACH could not be utilized.	A consumer is ready to checkout at a merchant. The consumer's mobile device is equipped with a near-field communication (NFC) chip which allows the consumer to place the mobile device in proximity to a POS reader equipped with an NFC chip to initiate a payment. There is a secure element either in the mobile device itself or located in the cloud if Host Card Emulation (HCE) is used, which stores the payment credentials (card or bank account information or a tokenized version of them) that were provided by the consumer during the initial enrollment process, and communicates the information to the other device. The merchant uses the information to originate an ACH debit to the consumer's account using the POS SEC code.	The consumer is confirming/initiating the payment utilizing their mobile device based upon information/authorization provided during the enrollment process. The consumer may be prompted for authentication such as a PIN or password and additional and/or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the merchant's account at its financial institution will be credited. Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The merchant's company name will appear on the consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Mobile Proximity Payment at the Point of Sale - Cloud	Examples include Cumberland Farms, Flash Foods and Spinx and examples of Service Providers include Zipline and Linked2Pay	A consumer is ready to checkout at a merchant. The consumer uses his/her mobile device to open the downloaded application for that merchant at the point of sale (POS). The application verifies location (through geolocation and/or by requiring information such as store or pump number) and provides the consumer with the total amount. The consumer initiates a payment from within the mobile application based on payment credentials that were provided during the initial enrollment process. The merchant originates an ACH debit to the consumer's account using the POS SEC code. A third party is sometimes used for these types of transactions. The third party effects the transfer of funds from the consumer's account to the merchant's account using the split transaction model with two discrete ACH transactions: 1) a POS debit to the consumer's account to collect the funds for the bill payment, and 2) a CCD credit to send the funds to the merchant. The third party may offer additional risk management / funds guarantee capabilities to the merchant as part of the service.	The consumer is confirming/initiating the payment utilizing his/her mobile device based upon information/authorization provided during the enrollment process. The consumer may be prompted for authentication such as a PIN or password and additional and/or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the merchant's account at its financial institution will be credited. Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The merchant's company name will appear on the consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Mobile Check - POP	Not aware of any current users, but there are service providers planning a mobile POP solution for release in 2015.	A field merchant accepts a check at the time of service or exchange of goods. Prior to accepting payment, the field merchant presents the consumer with notice that the check will be converted. The notice can be displayed on a screen for the consumer to read, or provided on the invoice. The merchant provides the consumer with an invoice statement that includes authorization language for check conversion. The consumer signs the invoice statement and provides the field merchant with a check. The field merchant uses a mobile device to read the routing and account numbers on the MICR line of the check, and gives the consumer the voided check and a copy of the invoice statement/ receipt. The merchant originates a POP transaction to the consumer's account.	The use of a mobile device does not change the authentication and authorization requirements for the merchant. On the settlement date, the consumer's account at his/her financial institution will be debited and the merchant's account at its financial institution will be credited. The merchant's company name will appear on the consumer's bank statement.
Mobile Check - BOC	Examples of vendors offering this product include Aptys.	A field merchant accepts a check at the time of service or exchange of goods. Prior to accepting payment, the field merchant presents the consumer with notice that the check will be converted. The notice can be displayed on a screen for the consumer to read, or provided on an invoice. The consumer provides the merchant with a completed check, and the field merchant uses a mobile device to capture an image of the eligible source document and transmits it to the back office to determine if it is eligible for conversion and to generate the BOC entry to the consumer's account. The field merchant provides the consumer with a copy of the notice language and takes the paper check back to the office where it is securely stored until destroyed.	The use of a mobile device does not change the authentication and authorization requirements for the merchant. On the settlement date, the consumer's account at his/her financial institution will be debited and the merchant's account at its financial institution will be credited. The merchant's company name will appear on the consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Online Banking P2P with a mobile device	Financial Institutions (large and small)	A consumer uses a mobile device to access his/her financial institution's website via a mobile web browser or downloaded application. The consumer submits an instruction to send money to another individual, and enters information about the other individual, including his name, address, and his routing and account numbers. The financial institution initiates a WEB credit to the receiving consumer. If the consumer does not have the routing and account number information for the recipient, typically they can enter an email address and the financial institution will send the recipient an email explaining how to register their banking information to receive the money.	The consumer user authenticates using his/her online credentials at his own financial institution's website. The use of a mobile device does not change the authentication requirements for the financial institution, but additional and /or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the other consumer's account at his/her financial institution will be credited. (The financial institution may choose to use a good funds model, in which the debit to the consumer's account occurs before the credit is sent as a risk management tool.) Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The other consumer's name will appear on each consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Online Banking P2P with mobile device using Third Party Service Provider	Examples of Third Party P2P Service Providers for financial institutions include: Fiserv's Popmoney, FIS' PeoplePay and Sprig by CO-OP	In this variation, the financial institution does not host the P2P application itself, but instead contracts with a third party for the P2P service. When a consumer uses a mobile device to access his/her financial institution's website via a mobile web browser or downloaded application, the consumer is "handed off" to the website / application of the third party. (In some cases, instead of the third party hosting that section of the financial institutionl website, the financial institution will gather payment information and pass by file to the third party.) The third party effects the transfer of funds from the sending consumer's account to the receiving consumer's account using the split transaction model with two discrete ACH transactions: 1) a WEB debit to the sending consumer's account to collect the funds for the payment, and 2) a WEB credit to send the funds to the receiving consumer. If the consumer does not have the routing and account number information for the recipient, typically they can enter an email address and the Third Party Service Provider will send the recipient an email explaining how to register their banking information to receive the money.	The consumer user authenticates using his/her online credentials at his own financial institution's website. The use of a mobile device does not change the authentication requirements for the financial institution, but additional and /or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the other consumer's account at his/her financial institution will be credited. (The financial institution may choose to use a good funds model, in which the debit to the consumer's account occurs before the credit is sent as a risk management tool.) Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The other consumer's name will appear on each consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
P2P via Nonbank Provider	Examples include Venmo (part of PayPal), Nooch and Popmoney	The consumer has enrolled for P2P services with a non-bank provider. The consumer uses a mobile device to access the non-bank provider's website via a mobile web browser or downloaded application to send money to another person. The consumer enters the other person's mobile phone number, email address, or both. If the other consumer is not registered with the service, the P2P provider sends the recipient an email explaining how to register their banking information to receive the money. The service provider effects the transfer of funds from the sending consumer's account to the receiving consumer's account using the split transaction model with two discrete ACH transactions: 1) an ACH WEB debit to collect the funds from the sending consumer, and 2) an ACH WEB credit to send funds to the receiving consumer.	The use of a mobile device does not change the authorization and authentication requirements. The non-bank provider should employ the same level of authorization and authentication as it would for originating WEB online debits, but additional and /or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the other consumer's account at his/her financial institution will be credited. (The service provider may choose to use a good funds model, in which the debit to the consumer's account occurs before the credit is sent as a risk management tool.) Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The other consumer's name will appear on each consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
One Time or Spontaneous Internet Purchase – Customer has enrolled or registered and uses mobile device to initiate payment	Any online merchant who accepts payments from enrolled consumers as well as intermediaries such as Bill Me Later (now PayPal Credit)	A consumer shopping online with a mobile device is ready to checkout at a merchant. The consumer may or may not have ever purchased from the merchant before, but has previously registered /enrolled with the merchant. When the customer is presented with payment options (e.g., alternative payment methods, credit card or bank account), the customer selects bank account and initiates a payment based on payment credentials that were provided during the enrollment process. The merchant originates an ACH debit to the consumer's account using the WEB SEC code. A third party is sometimes used for these types of transactions. The third party effects the transfer of funds from the consumer's account to the merchant's account using the split transaction model with two discrete ACH transactions: 1) a WEB debit to the consumer's account to collect the funds for the bill payment, and 2) a CCD credit to send the funds to the merchant. The third party may offer additional risk management / funds guarantee capabilities to the merchant as part of the service.	The use of a mobile device does not change the authorization and authentication requirements; however, the authorization and part of the authentication process takes place during enrollment when the consumer authorizes the payments, not during the confirmation/initiation process. The Merchant/ Third Party should employ the same level of authentication as it would for online initiation, but additional and /or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the merchant's account at its financial institution will be credited. (If a third party is used, they may choose to use a good funds model, in which the debit to the consumer's account occurs before the credit is sent to the merchant as a risk management tool.) Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The merchant's name will appear on the consumer's bank statement.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
One Time or Spontaneous Internet Purchase – Customer has NOT previously enrolled or registered and uses mobile device to authorize payment	Any online merchant that accepts direct payment from a bank account such as Amazon.com	A consumer shopping online with a mobile device is ready to checkout at a merchant. The consumer may or may not have ever purchased from the merchant before. When the customer is presented with payment options (e.g., alternative payment methods, credit card or bank account), the customer selects bank account and enters his/her payment credentials and authorizes a debit to his/her account. The merchant originates an ACH debit to the consumer's account using the WEB SEC code. A third party is sometimes used for these types of transactions. The third party effects the transfer of funds from the consumer's account to the merchant's account using the split transaction model with two discrete ACH transactions: 1) a WEB debit to the consumer's account to collect the funds for the bill payment, and 2) a CCD credit to send the funds to the merchant. The third party may offer additional risk management / funds guarantee capabilities to the merchant as part of the service.	The use of a mobile device does not change the authorization and authentication requirements. The merchant should employ the same level of authorization and authentication as it would for originating online WEB debits, but additional and /or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the consumer's account at his/her financial institution will be debited and the merchant's account at its financial institution will be credited. (If a third party is used, they may choose to use a good funds model, in which the debit to the consumer's account occurs before the credit is sent to the merchant as a risk management tool.) Confirmation of the payment is typically delivered to the consumer via SMS/text or email, but can be delivered by other methods designated by the consumer. The other merchant's name will appear on the consumer's bank statement.
Corporate Payments - Payroll	Service is offered primarily by large financial institutions	A company representative uses a mobile device to log onto its financial institution's website's Online Banking / ACH Origination via a mobile web browser. The representative approves/confirms a previously created set of transactions to pay employees. The financial institution initiates PPD credits to the employees and a debit for the total to the company's account.	The use of a mobile device does not change the authorization and authentication requirements. The financial institution should employ the same level of authorization and authentication as it would for originating payroll in an online environment, but additional and /or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Management section of paper.) On the settlement date, the employee's account at his/her financial institution will be credited and the company's account at its financial institution will be debited.

Use	Companies Offering Service	Scenario	Authentication, Authorization and Settlement
Corporate Payments – trading partner payments	Service is offered primarily by large financial institutions	A company representative uses a mobile device to log onto its financial institution's website's Online Banking / ACH Origination via a mobile web browser. The representative approves/confirms a previously created set of transactions to pay trading partners. The financial institution initiates CCD or CTX credits to the trading partners and a debit for the total to the company's account.	The use of a mobile device does not change the authorization and authentication requirements. The financial institution should employ the same level of authorization and authentication as it would for originating credits to trading partners in an online environment, but additional and /or different methods may be used for authentication which take advantage of options available with a mobile device. (See Risk Mitigation section of paper.) On the settlement date, the trading partner's account at its financial institution will be credited and the company's account at its financial institution will be debited.