



## **Mobile ACH Payments**

*Request for Comment*

### **Executive Summary and Rules Description**

**September 1, 2009**

#### **REQUEST FOR COMMENT – RESPONSES DUE BY FRIDAY, OCTOBER 16, 2009**

NACHA requests comment on a proposal to amend the *NACHA Operating Rules* entitled “Mobile ACH Payments.” Comments are due by October 16, 2009.

This proposal may have business and technology impacts that go beyond those typically considered in a Request for Comment. NACHA specifically requests that interested parties circulate this RFC and help obtain input from organizations and departments that may be impacted, but that may not typically respond to RFCs. For financial institutions, this could be from areas responsible for technology, retail and online banking, and legal.

#### **NACHA STAFF CONTACTS**

Return comments to:

Maribel Bondoc, Manager, Network Rules

Fax: (703) 787-0996

E-mail: [mbondoc@nacha.org](mailto:mbondoc@nacha.org)

Questions:

Julie Hedlund, Senior Director, Network Rules

Phone: (703) 561-1100

E-mail: [jhedlund@nacha.org](mailto:jhedlund@nacha.org)

Michael Herd, Managing Director, ACH Network Rules

Phone: (703) 561-3924

E-mail: [mherd@nacha.org](mailto:mherd@nacha.org)

#### **Part I: Proposal Brief**

This *Rules* proposal (“Rule”) would establish a framework in the *NACHA Operating Rules* (“*Rules*”) for mobile payments. The Rule would expand the definition of Internet-Initiated Entries (WEB) to include ACH debits authorized and/or initiated via mobile (wireless) networks<sup>1</sup> and require that those payments utilize the WEB Standard Entry Class (SEC) code.

---

<sup>1</sup> The use of the term “mobile” in this RFC pertains to payments made with a mobile device such as a smart phone, cell phone, and/or PDA where the payment information is transmitted via a wireless network as defined in this Rules proposal. This RFC often uses the term mobile instead of wireless since mobile is the common industry vernacular used to describe both the devices and the payment channel.

Because mobile payments have only recently emerged, the *Rules* do not currently address them specifically. Many companies, however, are either originating these payments over the ACH Network already or plan to in the near future. Including mobile payments within the definition of WEB would provide a framework in the *Rules* for the proper authorization and authentication of these payments, and extend the security and risk management provisions of WEB to mobile payments.

Specifically, this proposal would:

- Expand the definition of WEB Entries to include debit entries authorized and/or initiated via Wireless Networks;
- Revise the definition of Unsecured Electronic Network to include wireless networks and provide additional clarification to the industry;
- Provide a definition of Wireless Network;
- Apply all provisions of the WEB SEC Code to mobile debit entries; and
- Revise the requirements for Transmission of ACH Information via Unsecured Electronic Networks to clarify that voice or keypad inputs over a wireless telephone to a live operator or VRU would not be subject to the requirement to secure the connection with a minimum of 128-bit RC4 encryption.

NACHA intentionally kept this Rules proposal narrowly focused on providing clarification to the industry on which SEC Code to use for mobile payments and to apply the authorization, risk management and security provisions of WEB to mobile payments. At the same time, NACHA recognizes that the mobile channel is a distinct delivery channel for payments with unique characteristics that may warrant additional rules in the future. Mobile payments, while growing rapidly, are still in their infancy. This Rule aims to balance the need to mitigate the risks of mobile ACH payments with the desire to remain flexible and to avoid prematurely adopting rules that might create unnecessary barriers to entry and/or stifle innovation and growth in the mobile payment industry. Accordingly, NACHA proposes this Rule as a short-term approach.

As a long-term approach, NACHA will continue to monitor, evaluate, and analyze mobile ACH payments and their impact upon the ACH Network. The focus of this Request for Comment is on the short-term approach, but NACHA also asks that interested parties provide input on a few questions related to a longer-term approach for mobile ACH payments.

## **Part II: Background**

This Rule proposal incorporates research and analysis on mobile payments conducted by NACHA's Cross-Council Mobile Banking Work Group ("Council").<sup>2</sup> The Council established the following goals:

- Identify unique risk considerations for mobile payments;<sup>3</sup>

---

<sup>2</sup> The Council includes representatives from all of NACHA's industry councils, with experts from financial institutions, RPAs, mobile carriers, telecommunications companies, security providers, payment processors, federal and state government employees and research analysts.

<sup>3</sup> For purposes of this RFC, "unique risks" mean those that apply to the mobile channel exclusively, over and above those that apply to both mobile and other remote payments, such as Internet payments.

- Conduct an analysis to determine how mobile ACH payments are currently being originated;
- Develop recommendations for the *Rules* as applied to mobile ACH payments, specifically in the area of risk management; and
- Evaluate the long-term impact of mobile payments on the ACH Network.

The Council found that Originators are using a variety of SEC Codes to originate mobile payments - PPD, WEB, TEL and CIE - with varying interpretations of how the existing *Rules* apply in a mobile environment. The Council also identified several unique characteristics and risks related to mobile payments, including:

- Mobile devices are small and portable, and easily lost, stolen, or used by someone not authorized to make payments on the device-owner's account;
- Mobile payments are often "multi-channel," meaning they can be authorized in one channel and initiated in another<sup>4</sup>;
- Three different customer-facing business models exist for mobile payments, each with different security and risk ramifications:
  1. Short Message Service (SMS)/text;
  2. mobile web browser; and
  3. dedicated payment applications downloaded to a smart phone;
- Mobile devices have small screens which could restrict Originators' ability to ensure adequate provision of authorization disclosures.

Based upon these findings, the Council proposed to amend the *Rules* for mobile ACH debit payments, and recommended that the Originator obligations contained within the WEB rules be applied.<sup>5</sup>

### **Part III: Justification for the Proposal**

While current mobile payment volume is low, industry analysts predict significant growth over the next five years as more consumers acquire smart phones and payment solution providers begin marketing more aggressively. Insight Research Corporation estimates that 2.2 billion consumers will generate \$124 billion in financial transactions by 2014.<sup>6</sup> A more conservative estimate still predicts huge growth: Mercator Advisory Group estimates that payments from remote devices will grow from an estimated \$389 million in 2009 to \$8.6 billion in 2014.<sup>7</sup>

The threat of attacks on mobile payments is low today compared to the online world, but mobile malware does exist. As the market matures and a dominant operating system (OS) emerges, the mobile market will be subject to the same level of threat as the traditional Internet is today. In its 2008 study on Mobile Banking Security Standards, Javelin Strategy & Research noted that once

---

<sup>4</sup> For example, a consumer might provide an authorization for multiple payments online, but then initiate the debit entry each month by typing a "yes" message using SMS/text via a smart phone.

<sup>5</sup> The Originator Obligations for WEB are to 1) Verify the Identity of the Receiver; 2) Deploy a Fraudulent Transaction Detection System; 3) Verify the RTN; and 4) Conduct an Annual Security Audit

<sup>6</sup> [http://banktech.com/channels/showArticle.jhtml;jsessionid=KBKUNWE5OVP2GQSNLRSKH0CJUNN2JVN?articleID=216900450&\\_requestid=1456442](http://banktech.com/channels/showArticle.jhtml;jsessionid=KBKUNWE5OVP2GQSNLRSKH0CJUNN2JVN?articleID=216900450&_requestid=1456442)

<sup>7</sup> [http://www.paymentsnews.com/mercator\\_advisory\\_group/](http://www.paymentsnews.com/mercator_advisory_group/)

professional fraudsters “...turn their attention to the mobile channel, we can expect an environment characterized by varied, determined, and sophisticated attacks.”<sup>8</sup>

Indeed, mobile payments share many of the characteristics and risks of other remote payments, such as WEB entries. A *Rules* framework would facilitate the growth of mobile ACH payments while simultaneously addressing risks to the Network and participants. Should mobile payments continue their rapid growth in the absence of rules and a serious security breach occurs, it might be considered a liability for NACHA and damage the reputation of the ACH Network.

ACH participants also need clarification on how to apply the *Rules* to mobile payments. Even among well-intentioned Network participants, the absence of specific rules for mobile ACH payments creates an environment for participants to apply their own interpretation of existing rules to their products and business models. This leads to greater industry confusion due to multiple and possibly conflicting interpretations of existing rules.

This Rule is intended to standardize the use of the WEB SEC Code for mobile payments while providing basic risk management and security standards to govern those payments. By taking a short-term and long-term approach, this Rule attempts to strike a balance between the need to provide clarity to the industry and manage risk while refraining from setting new and restrictive rules that might stifle the growth and development of mobile payments.

#### **Part IV: Impact of the Proposal**

##### ***Benefits of the Proposal***

Redefining and applying the WEB SEC Code to mobile payments would provide much needed clarification to ODFIs, RDFIs, Originators and third parties about how to apply the *Rules* to these payments. Standardizing the use of the WEB SEC Code and applying the risk management and security provisions of WEB to mobile payments would create a more stable environment within which to develop payment products and services while reducing the inherent risks.

By channeling mobile payment volume to the WEB SEC Code, this Rule would enable ODFIs to conduct more effective risk management by monitoring WEB volume and activity for their Originators of mobile payments. ODFIs could revisit their exposure limits with Originators that choose to offer mobile payment services. The Rule would thus reduce ODFIs’ credit, fraud, operational and reputation risks related to mobile payments and the associated costs of exception processing and dispute resolution.

The Rule would provide RDFIs with additional tools for customer service and for managing the dispute resolution process because they could pinpoint any mobile payment disputes or exceptions to a single SEC Code – WEB.

Finally, a discrete set of *Rules* for mobile payments would enable Originators and Third Party Service Providers to implement internal processes and procedures for these entries in order to improve operations and customer service, reduce risk and fraud, and minimize exceptions and disputes.

---

<sup>8</sup> Javelin Strategy and Research: 2008 Mobile Banking Security Standards Report.

### ***Costs to Comply with the Proposal***

The anticipated costs to comply with this Rule are limited for both ODFIs and RDFIs since no major software changes are anticipated. ODFIs would bear costs associated with reviewing their WEB exposure limits and their agreements with Originators that originate mobile payments. ODFIs would also bear costs related to educating their Originators on their WEB Entry obligations as they apply to mobile payments. Both ODFIs and RDFIs would bear some customer service and training costs associated with the Rule.

For Originators and Third-Party Service Providers, costs will vary depending on their experience with the ACH Network and whether or not they are already originating WEB entries. The major cost of this Rule for Originators and TPSPs would be in compliance with the security and risk management provisions contained within the Originator obligations for WEB entries. Seasoned Network participants that have already deployed a Fraudulent Transaction Detection System, implemented a commercially reasonable method to verify the Receiver's identity, and conduct annual security audits for other ACH applications are not likely to incur significant cost to comply with the Rule. For new participants that have never originated ACH payments, the cost could be significant, but would be similar to costs they would incur for implementing ACH payments without this rule change. In spite of those costs, it is especially these new participants that need to be aware of the Originator obligations and how to apply them.

## **Part V: Rules Framework and Implementation**

### ***Elements of the Proposal***

- The *Rules* would expand the definition of Internet-Initiated Entries (WEB) to include payments authorized or initiated via a wireless (mobile) network.
- The definition of Unsecured Electronic Network would be revised to include wireless networks and provide additional clarification to the industry.
- A definition of Wireless Network would be added.
- The existing Obligations of Originators for WEB Entries would be applied to mobile payments; and
- The section on Transmission of ACH Information Via Unsecured Electronic Networks would clarify that voice or keypad inputs made via a wireless telephone to a live operator or VRU would not be subject to the requirement to provide security equivalent to 128-bit RC4 encryption.

### ***Definition of WEB Entry***

This proposal would modify the *Rules* to define a WEB Entry as a debit entry to a Consumer Account based upon an authorization obtained from a Consumer via the Internet or a Wireless Network. In addition, the WEB Rules would apply to individual debit payments initiated via a Wireless Network regardless of the form of the original authorization.<sup>9</sup> Many SEC Codes are determined on the basis of where the authorization is obtained; because mobile ACH payment

---

<sup>9</sup> For example, if a Consumer signed a paper authorization for a mobile payment service, but initiated each individual debit via a SMS/text message or through a dedicated mobile payment application, that payment would be a WEB Entry.

processing is in its earliest stage, however, there is a need to more fully understand their associated risks. Therefore, this Rule would require mobile debit payments to be handled as “WEB” not only when the original authorization is obtained via the Internet or Wireless Network, but also when subsequent debits are initiated via a Wireless Network, regardless of the original form of authorization.

Anecdotal research suggests that this Rule is unlikely to have a material impact on the use of SEC codes because Originators most often enroll customers or obtain authorization for mobile payments via a web site, which would require the use of the WEB SEC Code anyway. Given the early stage of development of such services, however, it seems advisable to take the broadest path to identifying mobile transactions before systems become entrenched using other SEC Codes and to ensure the application of the risk management and security provisions for WEB. NACHA specifically requests comment on whether the industry agrees that payments both authorized and/or initiated via the mobile channel should be originated as WEB entries and also whether this same standard should apply to Internet-initiated entries for consistency and improved risk management within the rules for WEB.

#### ***Definition of Wireless Network***

The Rule also provides a definition of Wireless Network as a wireless communication network, but excludes local area networks that are secured, at a minimum, with the equivalent of 128-bit RC4 encryption. NACHA requests comment on whether this definition is adequate, and whether excluding local area networks creates additional risk to the Network.

#### ***Definition of Unsecured Electronic Network***

The definition of Unsecured Electronic Network includes one substantive change, which is to clarify that these networks can be “wired or wireless.” The other revisions to the definition are intended solely to provide clarification that a virtual private network (VPN) that uses sufficient encryption is not included in the definition of Unsecured Electronic Network. NACHA requests comment regarding whether this revised definition provides adequate clarification.

#### ***Obligations of Originators of Internet and Mobile Entries***

The Rule applies the existing Originator Obligations for WEB entries to mobile payments.

These obligations include:

- deploying a commercially reasonable fraudulent transaction detection system to screen each entry;
- deploying a commercially reasonable method of authentication to verify the identity of the Receiver;
- using a commercially reasonable procedure to verify that routing numbers are valid; and,
- conducting an annual security audit.

NACHA requests comment on whether these Obligations, as currently stated in the *Rules*, are adequate to address the existing risks of mobile payments as they are understood today.

#### ***Transmission of ACH Information Via Unsecured Electronic Networks***

This section of the *Rules* (Section 1.6) specifies that the transmission of any ACH Information via Unsecured Electronic Networks must be encrypted with a minimum of 128-bit RC4 encryption. Currently, this section excludes “(t)ransmissions or exchanges of banking

information over an Unsecured Electronic Network by means of voice or keypad inputs from a wireline or wireless telephone...unless the telephone is used to access the Internet.”

This exception was not crafted with mobile payment services in mind, but rather was designed to avoid unintended consequences for traditional bank customer service operations that may include communication of ACH-related information. In order to ensure that this exception does not apply to wireless networks, the section has been revised to state that voice or keypad inputs from “a wireline or wireless telephone to a live operator or voice response unit” are exempted from the rule. NACHA requests comment on whether the revision captures the difference between the use of wireless telephone for purposes of initiating payments and for customer service applications.

## **Part VI: Other Issues**

### ***Mobile SEC Code***

In its research, the Council defined several compelling reasons to create a dedicated SEC Code for mobile payments. A mobile SEC code would enable NACHA to craft rules that are specific to any unique characteristics of mobile payments. It would also enable financial institutions to track and monitor their mobile payments volume and apply appropriate risk management measures. NACHA and all Network participants would be able to determine the overall volume of mobile payments in the Network.

In conducting further research, however, NACHA found that many industry participants are wary about the need for a new SEC code at this time. Several financial institutions suggested that because the mobile payments industry is so nascent, they do not yet know whether the unique characteristics of mobile payments will increase or reduce risk. For example, although SMS/text messages are unencrypted, they can also be used to provide real-time fraud alerts and payment confirmations which may in fact reduce risk. They suggested that imposing a new SEC Code upon such a new payment mechanism could increase the cost of mobile payments without a certain return on that investment in the form of reduced risk and fraud.

In addition, security experts indicated that the security of mobile web browsers are comparable to that of desktop browsers, making ACH payments made from a mobile web browser virtually identical to Internet-initiated WEB entries. With regard to payments made from dedicated mobile applications, the volume is currently too low to determine whether the risks justify the cost of applying a new SEC Code.

In discussions with other payment networks, NACHA discovered that while the card networks and online debit networks are closely monitoring mobile payments, they have not yet applied separate rules for mobile payments.<sup>10</sup> For example, mobile credit card payments fall within the category of “card-not-present.” If NACHA created a strict set of *Rules* for mobile payments and applied a new SEC Code, it would be inconsistent with the current approach taken by other payment networks.

Despite differing opinions about creating a new SEC Code, the Council and all other experts NACHA consulted agreed that it made sense to apply the risk management and security

---

<sup>10</sup> With the exception of branded product offerings such as P2P payment services

provisions for WEB entries to mobile payments, and continue to monitor, research, and evaluate mobile payments as they evolve. As a result, this Rule constitutes a short-term approach by including mobile payments within the definition of WEB entries, applying all of the existing security and risk management provisions of WEB to mobile payments, and revising the sections referring to an Unsecured Electronic Network to ensure they included wireless networks.

The long-term approach involves continuing evaluation to determine whether a new SEC Code will be needed in the future or, in the absence of an SEC Code, another method for tracking mobile payment volume. NACHA will continue working with the Council and the Product Group for Mobile Payments to evaluate other potential issues, including but not limited to:

- New SEC Code for mobile payments;
- Tracking mobile payment volume;
- Use of unencrypted SMS in payment applications;
- Storage of banking information on mobile devices;
- Provision of authorization disclosures via mobile devices;
- Security and use of Dedicated Applications for mobile payments;
- How PCI compliance might be applicable to mobile and other ACH payments;
- Mobile credits and mobile P2P payments.

NACHA requests comment on two issues related to the application of an SEC Code to mobile payments: 1) Do industry participants believe that the unique characteristics and risks of mobile payments will eventually warrant a separate SEC Code; and 2) In the absence of a separate SEC Code, how do Network participants plan to track mobile payments volume? Are there other methods of tracking that NACHA should consider for inclusion within future *NACHA Operating Rules*?

### ***Mobile Devices***

Mobile devices are portable, can be lost or stolen, and can also store sensitive information such as banking or consumer-level ACH information. This could lead to opportunities for fraud. Should NACHA consider rules that address some of these risks directly, such as prohibiting the storage of ACH information on mobile devices? What other rules should NACHA consider with respect to the use of mobile devices for payments?

### ***Authorization Disclosures on a Small Screen***

NACHA is seeking input from Originators of mobile payments on how they provide authorization disclosures via a mobile device. Is the language shortened and simplified to fit the small screen and/or are the disclosures being provided in another channel, such as a link to a website or in the mail?

### ***SMS/Text Payments***

By incorporating wireless network into the definition of Unsecured Electronic Network, the Rule would have the effect of applying the minimum encryption/secure transmission standard of the *Rules* (Section 1.6) to SMS/text messages. Because SMS/text messages do not include native encryption, their use for transmitting banking information to initiate an ACH debit would not be supported by the *Rules*.

Some financial institutions already allow customers to initiate or confirm a pre-arranged payment by acknowledging or responding to a text message, even when the text message itself does not carry any banking information. Given the possibility of a person other than the account holder responding to an SMS alert requesting permission to initiate a payment, NACHA requests comment whether the Originator should be required to re-authenticate the Receiver each time a payment is initiated via a SMS response.

### ***Mobile ACH Credit Payments***

This Rule concerns ACH debit payments authorized or initiated via a wireless network. Financial institutions, however, may also allow consumers to initiate ACH credit payments (i.e., CIE entries) out of their deposit accounts, either through mobile access to the financial institution's online banking platform (e.g., mobile browser), via a dedicated smart phone application, or by sending or responding to an SMS/text message. In any case, the minimum encryption/secure transmission standard of the *Rules* (Section 1.6) would apply to banking information transmitted between the consumer and the financial institution; otherwise, this Rule does not propose any amendments to the NACHA *Rules* regarding mobile-initiated ACH credit payments. Appropriate origination, risk management, and data security measures would be at the discretion of the financial institution, just as they are for ACH credit payments initiated via online banking and billpay.

### **Part VII: Technical Summary**

The following changes to the technical language within the *Rules* are included in this proposal:

- Article One, Section 1.6 (Transmission of ACH Information Via Unsecured Electronic Networks) would be expanded to clarify that transmissions or exchanges of banking information over an Unsecured Electronic Network by voice or keypad inputs from a wireless telephone to a live operator or voice response unit are not subject to the requirement for the use of 128-bit RC4 encryption technology.
- Article Two, Section 2.12 (Internet-Initiated Entries) – This section of the rules, which presently addresses the initiation of WEB entries, would be expanded to also include, within its scope, ACH transactions initiated via a mobile device. To reflect this change, the title of this subsection would be revised to read “Internet and Mobile Entries.”
- Article Two, Subsection 2.12.1 (General Rule) – The general rule related to WEB entries would be revised to require each Originator, Third-Party Sender and ODFI to utilize the WEB SEC Code to identify debit entries to Consumer Accounts as described in the definition of a WEB entry in subsection 14.1.72.
- Article Three, Section 3.9 (Obligations of Originators of Internet-Initiated Entries) – This section addressing an Originator's obligations with respect to the initiation of WEB entries would be revised to include, within its scope, the origination of transactions via a mobile device. To reflect this change, the title of this subsection would be revised to read “Obligations of Originators of Internet and Mobile Entries.”
- Article Five, Section 5.3 (Performance of ODFI Obligations) – The reference to Internet-Initiated Entries within this section would be revised to reflect the expansion of that section to include mobile payments.
- Article Fourteen, Subsection 14.1.71 (Unsecured Electronic Network) – The definition of an Unsecured Electronic Network would be revised to incorporate references to the use of both

wired and wireless networks using technology that does not meet the minimum standard of 128-bit RC4 encryption technology. This revised definition also clarifies that, while the Internet continues to be defined as an unsecured electronic network, a Virtual Private Network using sufficient encryption technology would not meet the definition of an Unsecured Electronic Network.

- Article Fourteen, Subsection 14.1.72 (“WEB entry” or “WEB”) – The definition of a WEB entry would be revised to include, within its scope, entries authorized via the Internet or a Wireless Network, as well as any entries initiated via a mobile device, regardless of the manner in which any underlying authorization for such entries was obtained (with the exception of an oral communication).
- Article Fourteen, Subsection 14.1.73 (“Wireless Network”) – A new definition would be added to define the concept of a wireless network as it relates to the NACHA Operating Rules.

### **Part VIII: Implementation**

An implementation date for this proposal of December 17, 2010 is recommended in order to standardize SEC Code usage for mobile ACH payments and to apply the risk management provisions of WEB to mobile payments in a timely manner. Because NACHA does not anticipate that this *Rules* proposal will require major software changes, the industry should have sufficient time to prepare for compliance with the provisions of these proposed rules.