Industry Update

DISCLAIMER

Macha, through its Direct Membership in Nacha, is a specially recognized and licensed provider of ACH education, publications and support.

Payments Associations are directly engaged in the Nacha rulemaking process and Accredited ACH Professional (AAP) program.

Nacha owns the copyright for the Nacha Operating Rules & Guidelines.

The Accredited ACH Professional (AAP) and Accredited Payments Risk Professional (APRP) is a service mark of Nacha.

This material is derived from collaborative work product developed by Nacha and its member Payments Associations and is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This material is not intended to provide any warranties or legal advice and is intended for educational purposes only.

This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein.

No part of this material may be used without the prior written permission of Macha/PAR.

© 2024 Macha/PAR All rights reserved

Macha EVERYTHING PAYMENTS - EVERYWHERE
PAYMENTS UNIVERSITY

Macha
EVERYTHING PAYMENTS - EVERYWHERE
PAYMENTS UNIVERSITY

Minor Topics Rule Changes

- General Rule/Definition of WEB Entries
- Definition of Originator
- Originator Action on Notification of Change
- Data Security Requirements
- Use of Prenotification Entries
- Clarification of Terminology – Subsequent Entries
- Effective Date: June 21, 2024

General Rule/Definition of WEB Entries

- General Rule for WEB Entries (Article Two, Subsection 2.5.17.1) and Definition of “Internet Initiated/Mobile Entry” (Article Eight, Section 8.55)
  - This re-words the WEB general rule and definition in Article Eight to make it clearer that the WEB SEC Code must be used for all consumer-to-consumer credits, regardless of how the consumer communicates the payment instruction to the ODFI or P2P service provider
  - While the rules already require all consumer-to-consumer credits to use the WEB SEC Code, the current reference to “Internet or Wireless Network” is confusing to some industry participants
    - Some ODFIs and P2P service providers are coding consumer-to-consumer credits as PPD entries when the consumer’s instruction has been communicated through non-internet means (e.g., via phone, in person)
  - Scope of change – Clarification of existing requirement on proper SEC Code use
  - Anticipated impact to industry participants – None for providers already compliant with the correct SEC Code requirement

Definition of Originator

- Definition of Originator (Article Eight, Section 8.71)
- Makes clarifying changes and alignments to the definitions of Originator:
  - Adds a reference to the Originator's authority to credit or debit the Receiver's account
  - Adds a notation to the definition of Originator that the Rules do not always require a Receiver's authorization (e.g., Reversals, Reclamations, Person-to-Person Entries)
- Prior to this amendment, the rules defined an Originator by the relationship it has with the ODFI – "a Person that has authorized an ODFI…to Transmit...an Entry…"
  - The existing definition is silent with respect to the Originator's obligation to have obtained the Receiver's authorization (when required by the Rules) to credit or debit the Receiver's account
  - By contrast, Receiver is defined as the party that has authorized the Originator to credit or debit an account
- The current definition of Originator is confusing to some industry participants when analyzing Originator versus Third-Party Sender relationships
- Scope of change – Clarification of intent - role of ACH participant
- Anticipated impact to industry participants – None

Originator Action on Notification of Change

- ODFI and Originator Action on Notification of Change (Article Two, Section 2.12.1)
- Gives Originators discretion to make NOC changes for any Single Entry, regardless of SEC Code
- The rules previously allowed the Originator discretion on whether it will act on NOCs received with respect to ARC, BOC, POP, RCK, single-entry WEB, single-entry TEL, XCK
  - This list identifies SEC Codes that, by definition, are one-time entries, and those that previously required a single/recurring indicator within the entry
- Wording of this section was out of date and required minor modification for clarity and reflection of current business practice
  - NOC rules were silent as to whether an Originator has discretion to make NOC changes related to single entries bearing other SEC Codes (e.g., PPD, CCD, CTX, IAT); nevertheless, in practice and in enforcement situations, Originators and Nacha have supported uniform treatment of NOCs for any one-time entries, regardless of SEC Code
  - A previously-required flag to identify certain TEL and WEB entries as single entries is no longer required by the Rules, rendering any perceived difference between single-entry TELs and WEBs and other SEC Codes (PPD, CCD, CTX, or IAT entries) moot
- Scope of change – Clarification of intent; reflection of current business practice
- Anticipated impact to industry participants – None-to-nominal

Data Security Requirements

- Security Requirements (Article One, Section 1.6)
- This amendment clarifies that, once a covered party meets the volume threshold for the first time, the requirement to render account numbers unreadable remains in effect, regardless of future volume
- Rules require each non-consumer Originator that is not a participating DFI; each Third-Party Service Provider; and each Third-Party Sender to protect DFI account numbers by rendering them unreadable when stored electronically
- This requirement is threshold-based and begins to apply to covered entities once those participants' annual ACH origination or transmission volume exceeds 2 million entries for the first time
    - The rules include a grace period for newly-covered parties to address implementation issues (must comply by June 30 of the year after triggering the 2 million entry threshold)
- As currently worded, the reference to the grace period can be misinterpreted as giving relief from compliance for parties already covered by the rule (i.e., if volume falls below 2 million, the requirement no longer applies)
- Scope of change – Clarification of intent
- Anticipated impact to industry participants – None

Use of Prenotification Entries

- General Rule for Prenotifications (Article Two, Subsection 2.6.1) & Definition of Prenotification Entry (Article Eight, Section 8.81)
- Aligns the prenote rules with industry practice by removing language that limits prenote use to only prior to the first credit or debit entry
- The rules allowed Originators to transmit prenotification entries for account validation prior to initiating the first credit or debit entry to the Receiver's account
- Originators indicate a need to re-validate that certain accounts are open and can accept ACH entries, even after live entries previously have been transmitted (ex: re-validation of inactive or dormant accounts before renewed ACH activity)
  - Originators want the ability to use ACH Network-based account validation methods for this purpose
  - In practice, many Originators already use prenotes for re-validation, regardless of language limiting use to prior to the first live entry
  - The recent Rule on Micro-Entries does not limit validation to before first use
- Scope of change – Minor change to reflect current business practice
- Anticipated impact to industry participants – None-to-minimal

Clarification of Terminology – “Subsequent Entries”

- Replaces references to “subsequent entry” in the Rules sections identified below with synonymous terms to avoid any confusion with the new definition “Subsequent Entry”
- With the adoption of definitions and rules for Standing Authorization and Subsequent Entries, minor changes are needed to prenote and NOC language to remedy now-ambiguous references to the use of the non-defined phrase “subsequent entry”
- The changes replace “subsequent” with other synonymous terms – “future”, “additional”, and “another”
- Scope of change – Clarification of intent
- Anticipated impact to industry participants – None

Risk Management Topics

ACH Risk Management Topics

- This set of amendments to the Nacha Operating Rules are intended to reduce the incidence of successful fraud attempts and improve the recovery of funds after frauds have occurred
- This package includes amendments related to:
  - Fraud monitoring by all parties in ACH except consumers
    - ODFIs, Originators, Third-Parties
    - RDFI monitoring of inbound ACH credits
  - Funds recovery tools
    - Allowing RDFI returns for suspicious activity
    - Clarifying ODFI's ability to request a return
    - Exception to RDFIs' funds availability requirements
  - Standardized information
    - Entry Descriptions – PAYROLL, PURCHASE
  - Written Statement of Unauthorized Debit (WSUD) processes
    - Acknowledge ability of Receivers to claim unauthorized upon presentment
    - Prompt return of debit after receipt of completed WSUD
- Amendments have various effective dates ranging from October 1, 2024 through June 19, 2026.

Dates	Effective Dates for Rule Amendments
October 1, 2024	• Codifying Expanded Use of Return Reason Code R17 • Expanded Use of ODFI Request for Return/R06 • Additional Funds Availability Exceptions (for RDFIs) • Timing of Written Statement of Unauthorized Debit • RDFI Must Promptly Return Unauthorized Debit
March 20, 2026	• Fraud Monitoring (by ODFIs) • Fraud Monitoring (by [non-consumer] Originators, TPSPs, and TPSs with 2023 ACH origination volume of 6 million or greater) • ACH Credit Monitoring by RDFIs (with 2023 ACH receipt volume of greater than 10 million) • New Company Entry Descriptions – PAYROLL and PURCHASE
June 19, 2026	• Fraud Monitoring by (all other) [non-consumer] Originators, TPSP, and TPS • ACH Credit Monitoring by (all other) RDFIs

Codify Use of Return Reason Code R17

- This rule explicitly allows, but does not require, an RDFI to use R17 to return an entry that it thinks is fraudulent
- Such use is optional and at the discretion of the RDFI
- The rule retains the current requirement to include the descriptor QUESTIONABLE in the return addenda record for such use
- The amendment is intended to improve the recovery of funds originated due to fraud
- The Rules provide for using the return code that most closely approximates the reason for the return
  - Nacha guidance has been that R17 is likely the closest return code for incidents of potential fraud
- Effective date: Oct 1, 2024
  - Use is optional by RDFIs (i.e., no compliance obligation by the implementation date)

Expanded Use of ODFI Request for Return/R06

- This rule expands the permissible uses of the Request for Return to allow an ODFI to request a return from the RDFI for any reason
- The ODFI still indemnifies the RDFI for compliance with the request
- Compliance by the RDFI remains optional
- An RDFI's only obligation to the ODFI is to respond to the ODFI's request
  - Regardless of whether the RDFI complies with the ODFI's request to return the Entry, the RDFI must advise the ODFI of its decision or the status of the request within ten (10) banking days of receipt of the ODFI's request
- This rule is intended to improve the recovery of funds when fraud has occurred
- Effective date: Oct 1, 2024
  - Use is optional by ODFIs (i.e., no implementation or compliance obligations by the effective date)

Additional Funds Availability Exceptions

- This rule provides RDFIs with an additional exemption from the funds availability requirements to include credit ACH Entries that the RDFI suspects are originated under False Pretenses
  - The additional exemption provides RDFIs with a tool under the Rules regarding questionable entries
  - RDFIs are still subject to requirements under Regulation CC for funds availability
  - The rule is intended to improve the recovery of funds when fraud has occurred
  - The rule is not intended to otherwise alter an RDFI's obligation to promptly make funds available as required by the Rules. An RDFI cannot delay funds availability because it has not monitored an ACH credit; but it can delay funds availability if its fraud identification processes and procedures flags an entry
- Prior to this amendment, the Nacha rules provided RDFIs with an exemption from funds availability requirements only if the RDFI reasonably suspects the credit entry was unauthorized
- False pretenses will be defined in a bit

Additional Funds Availability Exceptions – Rules Language

- New Language
  - “An RDFI that reasonably suspects that a credit Entry is unlawful, involves the proceeds of unlawful activity, or is otherwise suspicious, including a credit Entry the RDFI suspects to be unauthorized or authorized by the Originator under False Pretenses, is exempt from the funds availability requirements of this Subsection 3.3.1. An RDFI invoking any such an exemption must take reasonable steps to promptly notify the ODFI.”
- The inclusion of “reasonable steps” is intended to acknowledge and accommodate circumstances in which it is not reasonable for an RDFI to promptly notify the ODFI; e.g., an event involving a large volume of entries
- Either the return of the Entry using R17 or contacting the ODFI would meet the notification requirement of the proposal
- Effective date: Oct 1, 2024

Timing of Written Statement of Unauthorized Debit (WSUD)

- This rule allows a WSUD to be signed and dated by the Receiver on or after the date on which the Entry is presented to the Receiver (either by posting to the account or by notice of a pending transaction), even if the debit has not yet been posted to the account
  - Through digital notifications and alerts, a consumer may be able to report an unauthorized debit prior to the debit posting to his or her account
  - Allowing such a debit to post after being reported may cause harm to the Receiver
- When a consumer account holder notifies an RDFI of an unauthorized debit, the RDFI must obtain a signed Written Statement of Unauthorized Debit (WSUD) to return the debit
  - Previously, the rules required that the WSUD be dated on or after the Settlement Date of the Entry
- This rule is intended to improve the process and experience when debits are claimed to be unauthorized
- The amendment does not otherwise change the requirement for an RDFI to obtain a consumer's WSUD
- Effective Oct 1, 2024

RDFI Must Promptly Return Unauthorized Debit

- This amendment requires that when returning an ACH debit as unauthorized or improper in the extended return timeframe, the RDFI must do so by the opening of the sixth Banking Day following the completion of its review of the receiver's signed WSUD
  - The amendment is intended to improve the recovery of funds and reduce the incidence of future fraud
  - The prompt return of an unauthorized debit alerts an ODFI and an Originator to a potential problem
  - This is also true in first-party fraud schemes in which the party who disputes the debit Entry is the same party who benefits from the original entry
  - A prompt return supports controls that an Originator may have enabled, such as a hold on funds or delayed shipment of merchandise
  - This amendment would not change reasons or requirements for obtaining a Written Statement of Unauthorized Debit
- Quick responses can be significant when responding to fraud. In the days immediately following posting of an unauthorized debit Entry, any delay in processing a return may expose the ODFI or Originator to additional risk

Now we are going to skip ahead a bit…

Standard Company Entry Descriptions

- The Company Entry Description is a 10-character field that the Originator uses to describe the purpose of a payment
  - There are required standards for specific Company Entry Descriptions defined in the Nacha Rules such as ACCTVERIFY, REVERSAL, HCCLAIMPMT, and RETRY PYMT
- Standardized uses of the Company Entry Description can help parties in the ACH Network identify, monitor and count the volume of payments for specific purposes; and can help manage risk
- Effective date: March 20, 2026, for both amendments
  - These are “no later than” dates, Originators may begin using the descriptions as soon as practical

Standard Company Entry Description - PAYROLL

- This rule establishes a new standard description for PPD Credits for payment of wages, salaries and similar types of compensation. The Company Entry Description field must contain the description PAYROLL
  - RDFIs that monitor inbound ACH credits will have better information regarding new or multiple payroll payments to an account
  - A standard description for payroll payments can help support RDFI logic to provide or suppress early funds availability
  - The amendment is intended to reduce the incidence of fraud involving payroll redirections

Standard Company Entry Description – PAYROLL – Rule Language

- New Language
  - “The use of the term “PAYROLL” in this field is descriptive and by use of the word, neither the Originator, nor the ODFI (or any Third-Party Service Provider acting on behalf of an Originator or ODFI), makes any representation or warranty to the RDFI or the Receiver regarding the Receiver’s employment status
- “The ODFI has no obligation to verify the presence or accuracy of the word “PAYROLL” as a description of purpose or employment status”

Standard Company Entry Description – PURCHASE – Rule Language

- This rule establishes a new standard description for e-commerce purchases; the Company Entry Description field must contain the description PURCHASE
- New Language
  - “For this purpose, an e-commerce purchase is a debit Entry authorized by a consumer Receiver for the online purchase of goods, including recurring purchases first authorized online. An e-commerce purchase uses the WEB debit SEC Code, except as permitted by the rule on Standing Authorization to use the PPD or TEL debit SEC Code.”
- “The ODFI has no obligation to verify the presence or accuracy of the word “PURCHASE” as a description of purpose.”

Fraud Monitoring by Originators, TPSPs and ODFIs

- This rule requires each non-Consumer Originator, ODFI, Third-Party Service Provider, and Third-Party Sender to establish and implement risk-based processes and procedures reasonably intended to identify ACH Entries initiated due to fraud
  - The amendment is intended to reduce the incidence of successful fraud attempts
  - Regular fraud detection monitoring can establish baselines of typical activity, making atypical activity easier to identify
- The Nacha rules currently require Originators to use a commercially reasonable fraudulent transaction detection system to screen WEB debits and when using MicroEntries
  - These rules are intended to reduce the incidence of unauthorized debits resulting from transactions initiated online, which can experience increased volume and velocity
  - The existing Nacha Board policy statement “urges that all participants implement adequate control systems to detect and prevent fraud.”

Fraud Monitoring by Originators, TPSPs, and ODFIs – Rules Language

- New language:
  - "Each Non-Consumer Originator, ODFI, and Third-Party Service Provider or Third-Party Sender acting on behalf of an Originator, Third-Party Sender or ODFI, must:
    - (a) establish and implement risk-based processes and procedures relevant to the role it plays in the authorization or Transmission of Entries that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses1; and
    - (b) at least annually review such processes and procedures and make appropriate updates to address evolving risks
- These processes and procedures do not require the screening of every ACH Entry individually, and do not need to be performed prior to the processing of Entries. An ODFI's processes and procedures may consider the processes and procedures implemented by other participants in the origination of Entries."

Guidance Examples

- A risk-based approach should not be used, however, to conclude that no monitoring is necessary at all; at a minimum, an entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions
- Monitoring transactions prior to processing provides the greatest opportunity for detecting and preventing potential fraud. However, this rule does not require such monitoring to be performed prior to processing Entries
- For transactions in which monitoring identifies as suspect, the ODFI can consider a number of actions. Actions may include, but are not limited to, stopping further processing of a flagged transaction; consulting with the Originator to determine the validity of the transaction; consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and contacting the RDFI to determine if characteristics of the Receiver's account raise additional red flags, or requesting the freeze or the return of funds

Fraud Monitoring by Originators, TPSPs and ODFIs – Effective Dates

- Effective dates:
  - Phase 1 – March 20, 2026
    - The rule applies to all ODFIs. • The rule applies to non-Consumer Originators, TPSPs, and TPSs with annual ACH origination volume of 6 million or greater in 2023 (this is the same volume threshold that was used in the recent ACH Data Security Rule – Phase 1)
  - Phase 2 – June 19, 2026
    - The rule applies to all other non-Consumer Originators, TPSPs, and TPSs

RDFI ACH Credit Monitoring

The rule amendment requires RDFIs to establish and implement risk-based processes and procedures reasonably intended to identify credit ACH Entries initiated due to fraud

- RDFIs have a view of incoming transactions as well as account profile information and historic activity on Receivers' accounts
- A risk-based approach to monitoring can consider factors such as transactional velocity, anomalies (e.g., SEC Code mismatch with account type), and account characteristics (e.g., age of account, average balance, etc.). This aligns with AML monitoring practices in place today
- Based on its monitoring of incoming credits, an RDFI may decide to return an entry or contact the ODFI to determine the validity of a transaction

This rule is intended to reduce the incidence of successful fraud and better enable the recovery of funds when fraud has occurred

- The rule aligns with an institution's regulatory obligation to monitor for suspicious transactions
- The rule does not require pre-posting monitoring of credit entries

RDFI ACH Credit Monitoring

- Historically, the RDFI has played a passive role in the ACH Network
  - The ODFI warrants that an Entry is authorized and that it complies with the Rules
  - The RDFI may rely solely on the account number for posting an Entry, and the RDFI may rely on Standard Entry Class Codes for the purpose of complying with the Nacha Rules
- Previously, the Nacha Rules required ODFIs to perform debit transaction monitoring, but did not apply transaction monitoring requirements to RDFIs
- Regulatory obligations for financial institutions require monitoring for suspicious transactions
  - Title 31 part 1020 establishes customer identification program (CIP) requirements and minimum anti-money laundering (AML) program requirements for FIs, including, but not limited to:
    - Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile
    - Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information

RDFI ACH Credit Monitoring –Rules Language

- New Rule language:
  - “Each RDFI must:
    - (a) establish and implement risk-based processes and procedures relevant to the role the RDFI plays in connection with the receipt of credit Entries that are reasonably intended to identify credit Entries that are suspected of being unauthorized or authorized under False Pretenses, including processes and procedures for responding when credit Entries are identified as potentially unauthorized or authorized under False Pretenses; and
    - (b) at least annually review such processes and procedures and make appropriate updates to address evolving risks
  - These processes and procedures do not require the screening of every ACH Entry individually, and do not need be performed prior to the processing of Entries.”

Guidance Examples

- An RDFI might take extra measures to detect fraud in transactions in which it has determined risks to be elevated; take basic precautions where it has determined that risks are lower, and exempt transactions or activities that it determines involve very low risk. A risk-based approach should not be used, however, to conclude that no monitoring is necessary at all; at a minimum, an entity applying a risk-based approach should conduct a risk assessment to identify and differentiate higher-risk from lower-risk transactions
- These risk-based processes and procedures do not require the screening of every ACH Entry individually, and they do not need be performed prior to processing Entries
- The requirement to establish processes and procedures reasonably intended to identify Entries suspected of being unauthorized or authorized under False Pretenses should not be interpreted to impose an obligation on RDFIs to prevent wrongful activity
- While an RDFI will not likely know the circumstances under which a credit Entry was originated, Entries that are unauthorized or authorized under False Pretenses potentially may be identified based on characteristics of the Entry and the receiving account, such as:
    - A Standard Entry Class Code that does not align with the type of receiving account, such as a corporate CCD entry to a consumer account
    - A high-dollar transaction that is atypical for the receiving account
    - A series of similar credit Entries received within a short period of time, such as multiple payroll or benefit payments
    - Any of the above to a new account, a dormant account, or to an account acting as a mule

RDFI ACH Credit Monitoring – Effective Dates

- Effective dates:
- Phase 1 – March 20, 2026
  - The rule would apply to RDFIs with annual ACH receipt volume of 10 million or greater in 2023
  - According to Nacha data from the 2023 ACH volume survey, this effective date would apply to about 175 RDFIs representing about 70% of ACH Network received volume
- Phase 2 – June 19, 2026
  - The rule would apply to all other RDFIs

No Changes to Liability; No Duties to Other Parties

- Both of the new fraud monitoring rules include language to address concerns that fraud monitoring requirements could be mis-interpreted as 1) re-allocating liability between ODFIs and RDFIs; and 2) establishing new duties to other parties to stop fraud
- New language
  - This [Subsection] does not modify or create, and shall not be interpreted to modify or create, in any way, rights or obligations of any Person under Article 4A. {For origination: An agreement to comply with the Rules or this [Subsection] does not, and shall not be interpreted to, constitute agreement to a "security procedure" for purposes of Article 4A unless otherwise specifically designated as such in an agreement with the ODFI.} The obligation to comply with this [Subsection] is enforceable solely by the National Association in accordance with Appendix Nine (Rules Enforcement) of these Rules and does not create or imply any other duty to any other Person
- This new language:
  - Explicitly disclaims modification of rights and obligations under UCC4A
  - Explicitly disclaims the creation of new duties to other parties
  - Explicitly states that enforcement is solely by Nacha
- Furthermore, the requirements of the new Rules do not modify or supersede the ODFI's warranty that the Entry is authorized

False Pretenses

- Several of the new rules also include references to a newly defined term, False Pretenses
- New language
  - False Pretenses “the inducement of a payment by a Person misrepresenting (a) that Person’s identity, (b) that Person’s association with or authority to act on behalf of another Person, or (c) the ownership of an account to be credited.”
- This definition covers common fraud scenarios such as Business Email Compromise (BEC), vendor impersonation, payroll impersonation, and other payee impersonations, and complements language on “unauthorized credits” (account takeover scenario). It does not cover scams involving fake, non-existent or poor-quality goods or services
- As a new definition, False Pretenses is also referred to in Rules language for Codifying Expanded Use of R17 and Additional Exceptions to Funds Availability.

False Pretenses

- Example of credit Entry not authorized by the Originator:
  - Account takeover - Fraudster gains access to the credentials necessary to initiate a transaction and initiates a credit entry from the accessed account. The accountholder (Originator) did not authorize the credit entry
- Examples of credit Entries authorized by the Originator under False Pretenses:
  - Receiver of the credit Entry misrepresents the Receiver's identity or ownership of the receiving account
  - Fraudster impersonates someone with the authority to order payment (e.g., a CEO/CFO via business email compromise) to induce someone with authority to originate a payment from the credit account to make a payment
  - Fraudster claims to be a vendor with whom the accountholder has a relationship and requests payment to fraudster's account
  - Fraudster claims to be a real estate settlement agent or attorney and requests funds transferred to fraudster's account
  - Fraudster claims to be an employee of an organizations and requests payment to fraudster's account; or, fraudster gains access to organization's payroll system and redirects payroll payments to fraudster's account

False Pretenses

- Examples of what is not considered an unauthorized credit Entry or a credit Entry authorized under False Pretenses:
  - A dispute regarding the quality or condition of, or warranties or timing of delivery for, goods or services (provided there are not other circumstances that would give rise to a claim of False Pretenses or unauthorized payment). For example, a business payment to a vendor, for which the quantity or quality of goods delivered is later disputed
  - Payment is made to the right person/organization but induced on a basis other than False Pretenses (e.g., a contribution to a charitable organization because it says they are going to spend the funds on something particular and then spends it on something else)

Questions?