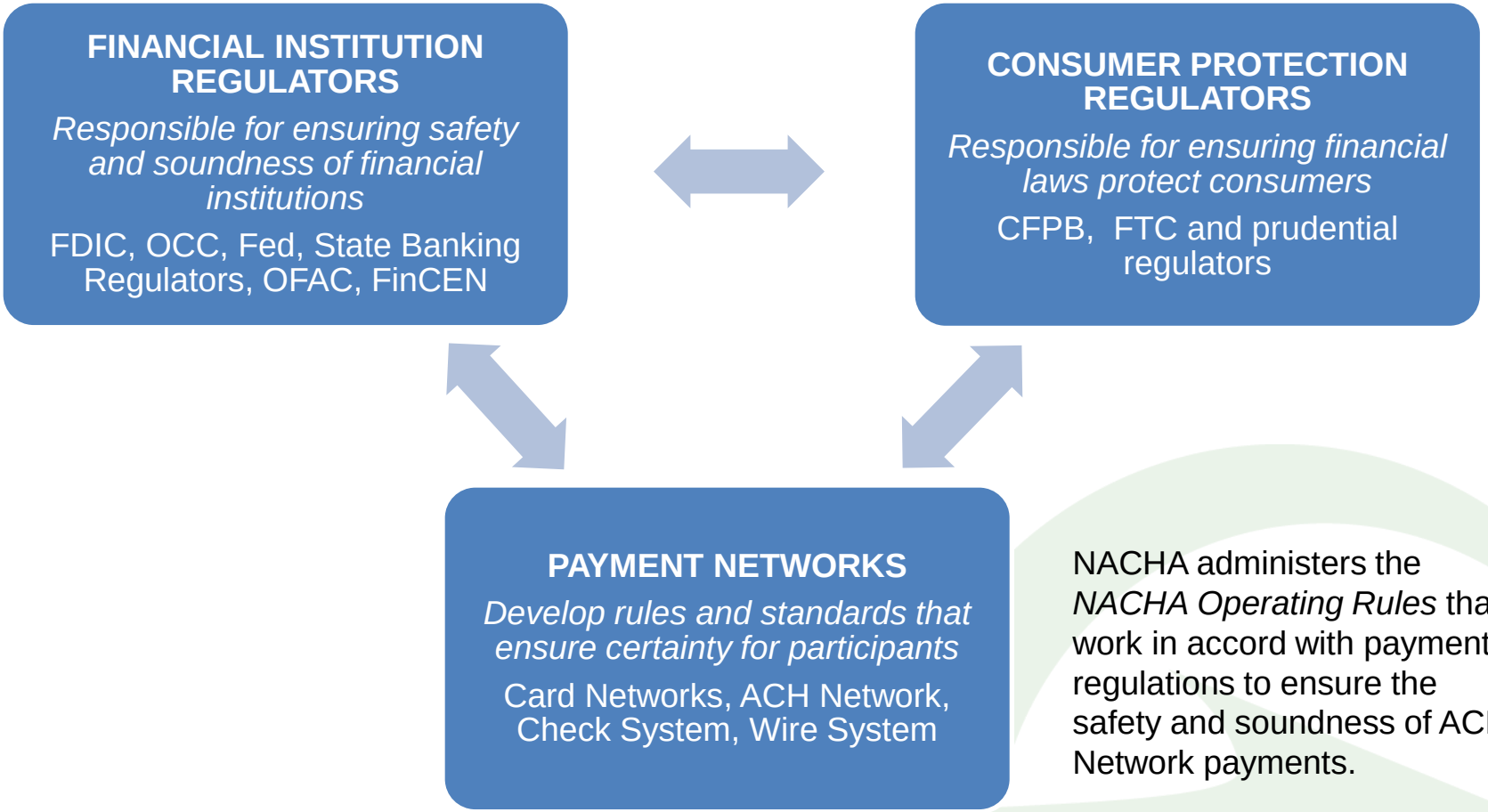
Legal and Regulatory Update
Executive Fraud Forum
Federal Reserve Bank of Atlanta

Jane Larimer
EVP ACH Network Administration
General Counsel
NACHA – The Electronic Payments Association
October 30, 2013

NACHA
The Electronic Payments Association®

A Network of Regulations and Authorities Govern Payments and Payments System Participants



NACHA administers the *NACHA Operating Rules* that work in accord with payment regulations to ensure the safety and soundness of ACH Network payments.

NACHA
The Electronic Payments Association®

Regulatory Guidance: Origination Activities

- OCC 2006-39: ACH Activities
- OCC 2008-12: Payment Processors
- FDIC FIL-3-2012: Revised Guidance on Payment Processor Relationships
- FDIC Supervisory Insights Summer 2011
- FinCEN FIN-2012-A010: Financial Advisory Risk Associated with Third Party Payment Processors
- FDIC FIL 43-2013
- FFIEC Exam Manual
- FFIEC IT Examination Handbook: Retail Payment Instrument Specific Risk Management Controls, ACH and Third-Party ACH Processing

FinCEN Advisory

- Risks Associated With Third Party Payment Processors
  - "Potential Red Flags for Illicit Use of Payments Processors:"
    - High numbers of consumer complaints and particularly high numbers of returns
    - TPPs maintaining accounts at multiple FIs
    - Consolidation Accounts – this may be a legitimate account – but TPPs can be used to conceal high return rates from ODFIs and regulators
    - Foreign located processors that process payment for telemarketers, online businesses and others
    - TPPs soliciting business with a distressed FI

FinCEN Advisory

- Risks Associated With Third Party Payment Processors (cont'd)
  - Guidance for FIs originating for TPPs:
    - FIs may need to update their anti-money laundering programs
    - FIs should determine during initial or ongoing due diligence whether:
      - external investigations or legal action are pending against a TPP or its owners
      - TPPs have obtained all necessary state licenses, registrations and approvals
    - FIs may need to file a SAR if they know, suspect or have reason to suspect that a TPP has conducted a transaction connected with illegal activity, including consumer fraud
      - Check the appropriate box on the SAR form, and include the term "payment "processor" in both the narrative portion and the subject occupation portion of the SAR

NACHA Operations Bulletin

- New York Times published an article on February 23, 2013, *Major Banks Aid in Payday Loans Banned by States*
  - "While the banks…do not make the loans, they are a critical link for the lenders, enabling the lenders to withdraw payments automatically from borrowers' bank accounts, even in states where the loans are banned entirely."
- ACH Operations Bulletin #2-2013: High Risk Originators and Questionable Debit Activity
  - Foundation: the ODFI is responsible for the valid authorization of all debits it initiates into the Network
  - Reminders of guidance that was previously issued in this area by the regulators, including OCC 2006-39
  - Elements of a robust risk management programs for ODFIs
  - RDFI responsibilities and practices
    - Responsibility to stop payment on one, multiple or all future debits
- ACH Operations Bulletin #3-2013: Reinitiation of Returned Debit Entries

Payday Lending

- The legality of the underlying transactions is in dispute: some payday lenders dispute the applicability of state law to online activity, and the tribes assert the sovereignty of federally recognized tribes
  - The ACH Network is caught in the cross-fire between payday lenders (including the tribes) and some regulatory entities
  - No regulatory expectation or NACHA Rule that requires an FI to know the legality of each underlying transaction – the expectation is to know the nature of the business of the originator and the risk it represents
  - RDFIs cannot screen, identify or block specific transactions
    - OFAC acknowledges the difficulty of screening domestic transactions
    - Reg GG
  - Lack of clear Federal direction or oversight

FDIC FIL-43-2013

FDIC Supervisory Approach to Payment Processing Relationships with Merchant Customers that Engage in Higher-Risk Activities:

- Issued September 27, 2013
- Clarifies FDIC's policy and supervisory approach for FIs that facilitate payment processing either directly or indirectly for higher risk merchant customers:
  - Perform proper risk assessments
  - Conduct due diligence to determine whether merchant customers are operating in accordance with applicable law, and
  - Maintain systems to monitor relationships over time
- Examination focus is on assessing wither FIs are adequately overseeing activities and transactions they process and appropriately managing and mitigating risks
- FI with appropriate systems and controls will not be criticized for providing payment processing services to businesses operating in compliance with applicable law

NACHA Rulemaking Initiatives

- Requests for Comment will be released on the following topics within the next several weeks:
  - Expanding the Network Enforcement Rules:
    - Lower threshold for unauthorized returns
    - Create new thresholds for administrative returns, and
    - Overall return rates
  - ACH Quality Fees
  - Reinitiation practices
  - Third Party topics

FinCEN Advisory

- Tax Refund Fraud and Related Identity Theft:
  - Issued to assist FIs with identifying tax refund fraud and reporting activity through the filing of SARs
  - The Advisory is intended to further the IRS' comprehensive strategy to prevent, detect and resolve tax-related identity theft crimes
  - Red Flag Examples:
    - Multiple refunds to different people are made to a single DDA
    - Opening multiple prepaid card accounts by one individual in different names using valid TINs – and subsequent mailing of the cards to the same address
    - Suspicious account opening on behalf of individuals that are not there, with the account opener being named as the signatory
  - FIs that know or suspect (or have reason to suspect) that a transaction involves proceeds from an illegal activity, is designed to evade the BSA, or lacks an apparent lawful purpose may be required to file a SAR
    - Use phrase "tax refund fraud" in the narrative section

NACHA Opt-In Program for RDFIs: IRS Refund Returns

- IRS and FMS requested NACHA's assistance in facilitating the recovery of questionable tax refunds sent via ACH
  - Previous IRS practice when receiving the return of an ACH credit (for example, due to incorrect account information) was to send a check
  - This practice assumed the tax return and refund are legitimate
  - IRS not able to validate tax return information against other data (e.g., W-2 statements) quickly enough
    - Under pressure to issue refunds as fast as possible
  - For fraudulent or other questionable tax refunds, the result is a lost opportunity to prevent loss of funds

NACHA Opt-In Program for RDFIs: IRS Refund Returns

- NACHA, IRS and FMS developed Opt-In Program for RDFIs
  - Provide a voluntary method for RDFIs to return ACH credits to IRS that does not automatically result in the issuance of a check
  - In cases of name mismatch between ACH entry and account record, the RDFI can return the ACH credit using the R17 return code
  - IRS normally receives near zero R17 ACH returns, so Opt-In Program returns are the only ones using R17
    - This unique identification allow IRS to segregate these ACH returns from other ACH returns
  - Available for 2012 tax filing season (beginning Jan 25)
  - Opt-In Program allows the voluntary use of a solution without the need to pass a rule that would require all RDFIs to implement

NACHA Opt-In Program for RDFIs: IRS Refund Returns

- Statistics as of September 11:
- 85 RDFIs participating
- 19,349 R17s have been sent, of which:
  - 11,843 (61%) were determined to be improper - $46,522,484.52 recovered ($3,928 average)
  - 7,506 (39%) were determined to be proper - $16,469,724.08 released ($2,194 average)

FFIEC: Statement and Proposed Guidance

- Statements versus Guidance:
  - An informational document versus the “thou shalts”
- Outsourced Cloud Computing Statement:
  - Issued on July 10, 2012, in response to questions received from FIs
  - Cloud computing is still a form of outsourcing with the same basic risk characteristics and risk management requirements as traditional forms of outsourcing
    - Third party vendor management guidance covers this as well – *see FFIEC Information Technology Examination Handbook* - especially the *Outsourcing Technology Services Booklet*
  - Remember – outsourcing does not relieve the FI of the obligation to ensure that the third party activity is conducted in a safe and secure manner!
    - A due diligence review must be performed, with thought given to:
      - How sensitive is the data that will be placed in the cloud? Is the data encrypted or protected?
      - Will the FI share data resources with data from other cloud clients? What controls are in place?
      - How will the provider respond to disasters and ensure continued service?

FFIEC: Statement and Proposed Guidance

- Social Media: Consumer Compliance Risk Management Guidance
  - Issued: January 23, 2013. Comments were due by March 24, 2013
  - The proposed guidance is intended to address the applicability of federal consumer protection/compliance laws to activities conducted via social media
    - Would apply to FIs – and non-bank entities supervised by the CFPB
  - Social Media defined as “a form of interactive online communication in which users can generate and share content through text, images, audio and video.”
    - Examples include Facebook, Twitter, Yelp, LinkedIn, etc.
    - Used for marketing, providing incentives, facilitating opening new accounts, engaging with existing and potential customers or providing loan pricing
  - Since tends to be informal and happens in a less secure environment, it presents unique challenges

FFIEC: Statement and Proposed Guidance

- Social Media: Consumer Compliance Risk Management Guidance risk management expectations :
  - FIs should have a risk management program that allows them to identify, measure, monitor and control social media risks
  - Risk areas include:
    - Compliance and legal risks:
      - Must follow all applicable laws and regs – translated into the social media environment (don't forget what you already know and do – and then translate)
    - Reputation risks including fraud and brand identity, consumer complaints and inquiries and employee use of social media sites
      - Remember users can post critical or inaccurate statements (!)
    - Operational risks includes the risk posed by an FI's use of IT
      - Social media platforms are vulnerable to malware

Questions and Contact Information

Jane Larimer
EVP ACH Network Administration
General Counsel
NACHA – The Electronic Payments Association
703.561.3927
jlarimer@nacha.org