Know Your Customer
&
Know Your Customer's Customers (KYCC)

BITS ACH Fraud Risk Subgroup

Presented by

George Thomas

November 19, 2008

Agenda

- Theme and Issue
- Types of Third Party Processors
- Risk from Third Party Merchant Processors
- Know Your Customer Procedures
- Know Your Customer's Customers Procedures
- Consequences

RADIX
CONSULTING
CORPORATION
the source for your payments needs

Prevent Fraudulent, Illegal and Questionable Activity

- Payments Systems Issues
  - Telemarketing Abuse and Fraud
  - Illegal Activity (Tobacco sales, Internet Gambling, Child Pornography, Ponzi schemes)
  - Questionable Business Practices (Payday Loans)
- Payment Instruments Used
  - ACH debits
  - Credit/Debit Cards
  - Demand Drafts
- Primary Cause
  - On-line Third Party Merchant Processors (over 90%)

Traditional Third-Party Processing

- Third-party
  - Originates and receives ACH transactions for financial institution directly to ACH Operator (e.g. Fiserv, NCR, EDS, etc)
  - Performs back-office operations (DDA posting, etc)
  - Payroll Processors (ADP, Paychex)
  - Bill Payment Providers (Checkfree)
- Financial institution
  - Responsible for all activity of the third-party processor in most cases without direct knowledge of what is submitted until settlement
  - Low risk: no history of abuse or fraud by traditional third party processors

Third Party Merchant Processor

Third Party Merchant Processor payment services:

The merchant sets up his store with products and pricing.   The payments for Internet or Telephone purchases are processed through the services of the Third Party Merchant Processor though it appears as if the actual merchant is doing the entire process. The actual merchant then becomes a supplier and the shipper of the goods.

Complex Third-Party Merchant Processor Arrangements

- One or more third party processors
- One or more Independent Sales Organizations (ISO)
- Originating for merchants and service providers unknown to ODFI

- **As an ODFI questions you need to ask:**
  - **Who are the originators?**
  - **What is their business?**
  - **Is it the type of originator you would do business with?**
  - **How are the authorizations obtained?**
  - **Third-party must apply same KYC policies as you would**

# Complex Third-Party Model - Who is your customer?
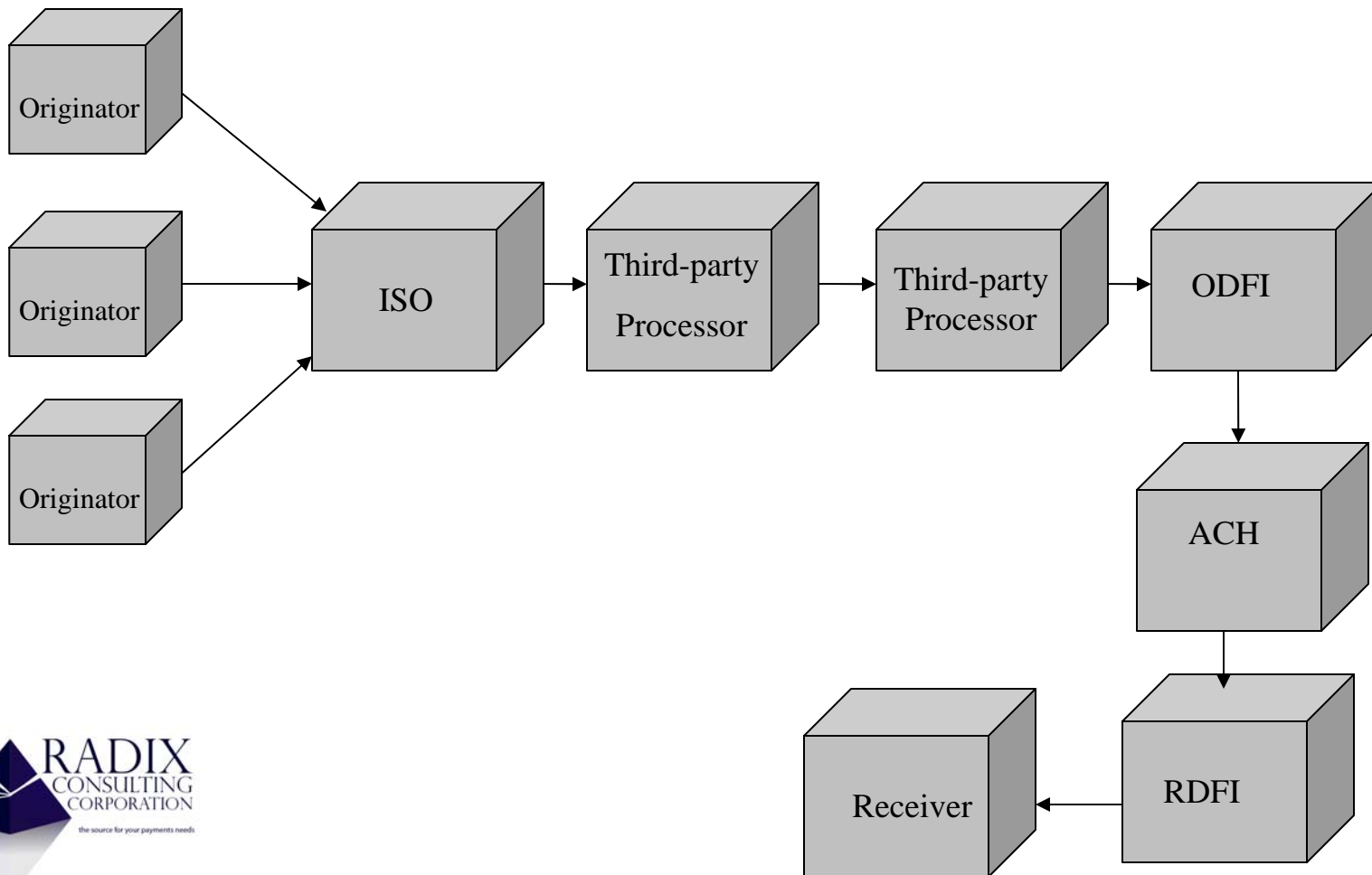
Worst Third-Party Payment Processor Model

- Third-party
  - Rents bank routing number and is directly connected to the ACH network
  - May originate ACH transactions for other third-party processors
  - Other third-party processors may submit transactions for many ISOs
- ODFI
  - Has no knowledge of forward or return activity until settlement
  - Thorough due diligence process on the third-party processor and know their customers
  - Risks are the same as the complex model but there is less control of the risks

Worst Third-Party Model - Who is your customer? What are they doing?
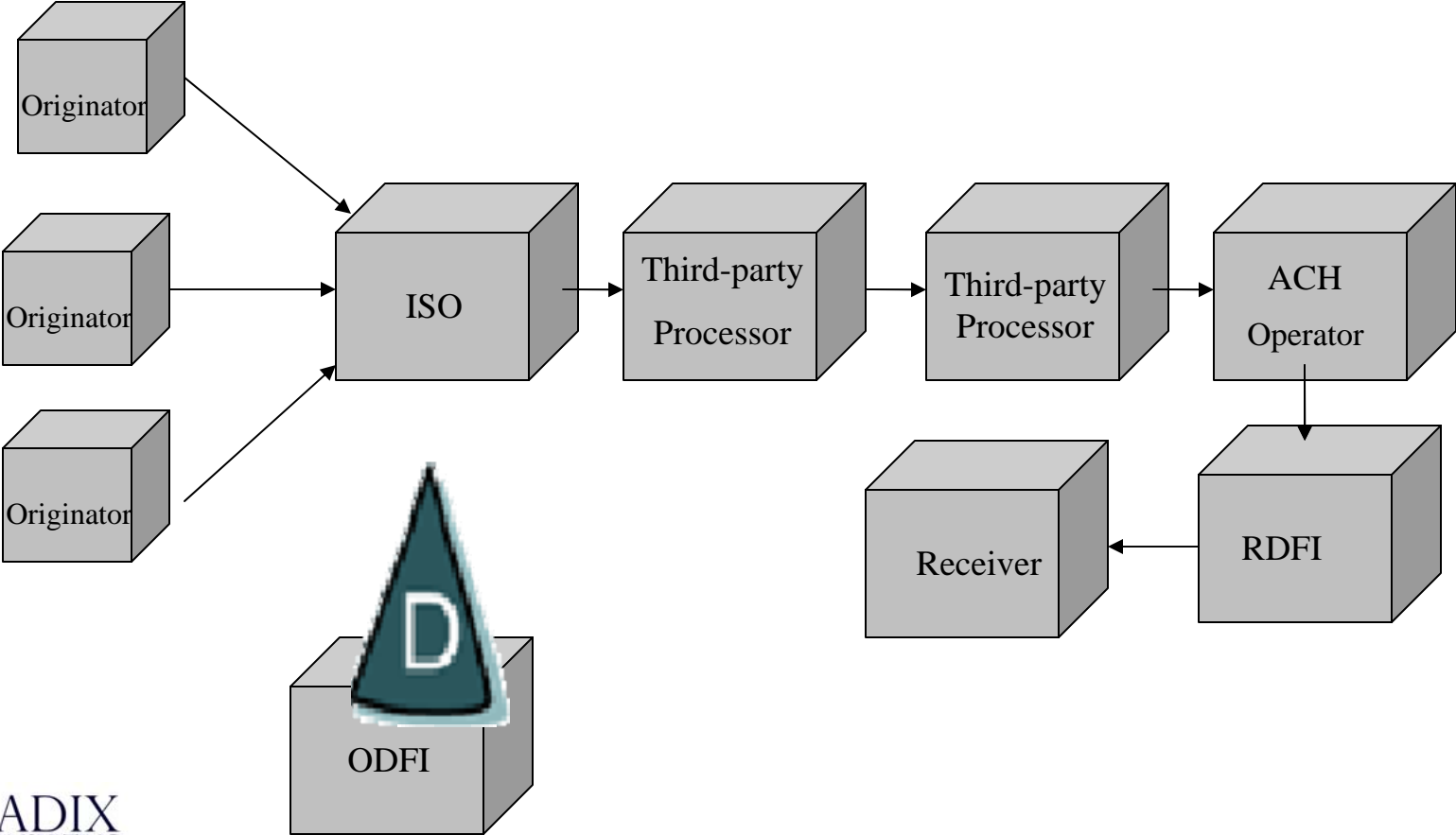
Financial Institution Risks from Third-Party Merchant Processor Arrangements

- ODFI Exposure
  - Credit risk – for customer funding
  - Return item risk – on debit transactions
  - Reputation risk
  - Breach of warranty – long term liability
  - ACH fraud loss

RADIX
CONSULTING
CORPORATION
the source for your payments needs

Know Your Customer

- Obtaining the Merchant's:
    - name (including all "doing business as" names),
    - address, phone number,
    - type of business or principal business activity,
    - taxpayer ID number, principals' names, principals' addresses, principals' phone numbers, principals' taxpayer ID numbers, geographic location,
    - web site address, and sales history;

Know Your Customer

- Conducting a background check of the Merchant and its principals by, at a minimum, doing the following:

  - reviewing the Merchant's web site, advertising, products, and services;

  - cross-checking the Merchant's provided information;

  - verifying the information provided by the Merchant with external agencies having the ability and expertise to provide such verification (e.g., the Better Business Bureau, Dunn & Bradstreet, etc.); and

  - validating the taxpayer ID numbers through income tax filings, incorporation documents, business papers and/or bank account information

Know Your Customer

- Reviewing the Merchant's sales history;
- Listing permissible standard entry class types, if applicable; and
- Using a unique company identifier for each Merchant or Third Party Merchant Processor and including the name of each Merchant or Third Party Processor (i.e., no acronyms, abbreviations or telephone numbers) for all transactions submitted for processing;
- Outlining Merchant termination procedures.

Know Your Customer's Customers

- Banks should require each Third Party Merchant Processor with which it does business *by agreement* to:
  - Identify each of the Merchants for whom the Third Party Merchant Processor would be originating transactions and provide the name of the company, address, type of business, telephone numbers and principals to the Bank at least semi-annually;
  - Identify all Secondary Third Party Merchant Processors that each Third Party Merchant Processor does business
  - Perform due diligence procedures described in the previous slides for each direct Merchant that the Third Party Merchant Processor processes for;
  - Require that each Secondary Merchant Processor that provides services for the Bank will perform the same due diligence as described in the Know Your Customer slides

Know Your Customer's Customers

- Require that all parties utilizing the ACH processing system be bound by the National Automated Clearing House Association ("NACHA") rules and that all transactions will be in compliance with all state and federal laws.

- Require that each Third Party Merchant Processor cease origination services for any Merchants or Third Party Merchant Processors that violate or do not meet the due diligence procedures of the Third Party Merchant Processor;

Know Your Customer's Customers

- Terminate Merchants and Secondary Third Party Merchant Processors that fail to:
    - Provide accurate Merchant information;
    - Notify the Third Party Merchant Processor Bank of new Merchants, independent sales organizations or other Secondary Third Party Merchant Processors;
    - Terminate Merchants that engage in activity that violates state or federal laws;
    - Terminate Merchants that switch ACH activity to demand drafts once notified of the problem; or
    - Terminate merchants that offer demand drafts to avoid ACH return scrutiny.

Know Your Customer's Customers

- Banks should perform the following verification procedures at least semi-annually:
  - Review Merchant listings provided by Third Party Merchant Processors;
  - Review company names and type of business for consistency; and
  - Perform background checks on a random sample of Merchants supplied by each Third Party Processor.

Consequences

- Subpoenas by law enforcement
- Assurances of discontinuance
- Adverse publicity
- Fines by regulators
- Fines by law enforcement
- Regulatory scrutiny
- Loss of Reputation

RADIX
CONSULTING
CORPORATION
the source for your payments needs

Questions

Thank You

Please visit www.radixconsulting.com for additional payments system articles