Crowe

Smart decisions. Lasting value.™

Electronic Banking

June 2019

Daniel Panduro

Presentation Overview

- Wire Transfer Process
- Automated Clearing House (ACH) Process
- Remote Deposit Capture (RDC) operations process
- Key Controls and Audit Points for the above
- Common findings that are frequently identified at our clients

ACH vs. Checks vs. Wires

	ACH	Checks	Wires
Returns	2-60 days	1-10 days	Irrevocable
Cost	Low	Medium	High
Float	None	1-3 days	None

Course Agenda

- Wire Transfers
- Automated Clearing House (ACH)
- Remote Deposit Capture (RDC)

Wire Transfers (Consumer Domestic Wire Example)

Customer

Phone, fax, etc.

Originating Bank

FedLine Advantage

$

Fed

FiServ - WireXChange

$

Beneficiary Bank

FiServ - Premier

Beneficiary

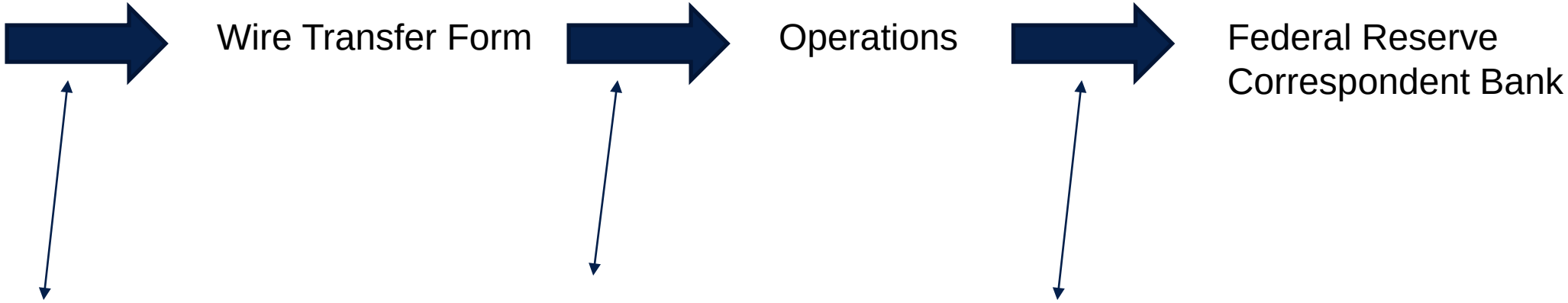
Fedwire Funds Service settles the funds between banks immediately

Has immediate Use of funds

Wire Transfer Process

Customers:

In Person
Fax
Email
Online



BSA/CIP/KYC/OFAC
Customer Signature
Call-Back Procedures

Customer Name, Address, Dollar Amount, Beneficiary, Name, Address, Routing Number, Account number, SWIFT Code

Input/Verify and Authorization

Wire Transfer Fraud

- Most corporate wire transfer fraud occurs through business email compromise.
  - In JP Morgan's 2019 Payments Fraud and Control Survey, 80% of surveyed financial institutions reported that their organization was exposed to business email compromise (BEC)

- Most consumer wire transfer fraud occurs through scams.
  - Common consumer scams target the elderly and include lottery or prize scams, debt collection scams, online dating scams, etc.

Key Controls

- Customer (internal users and external customers) validation
- Separate users for initiate, approve and release, with appropriate limits
- Hold on funds or debit to account
- Use of repetitive transfers wherever possible
- Volume and amount limits
- Tokens

Wire Transfer – Common Findings

- A callback is not performed or other security procedure not performed in accordance with established agreement
- The wire transfer form is not completed in entirety or accurately
- Proper approval is not obtained for sending the outgoing wire transfer
- Application specific:
  - Inappropriate privileged access to the wire system
  - A review of users' access is not performed
  - A review of administrative activity or pertinent activity is not reviewed
  - (FedLine) – Fedwire Funds Authorization Form (for processing offline wires) is not reviewed and approved annually
- Open discussion on other findings

Course Agenda

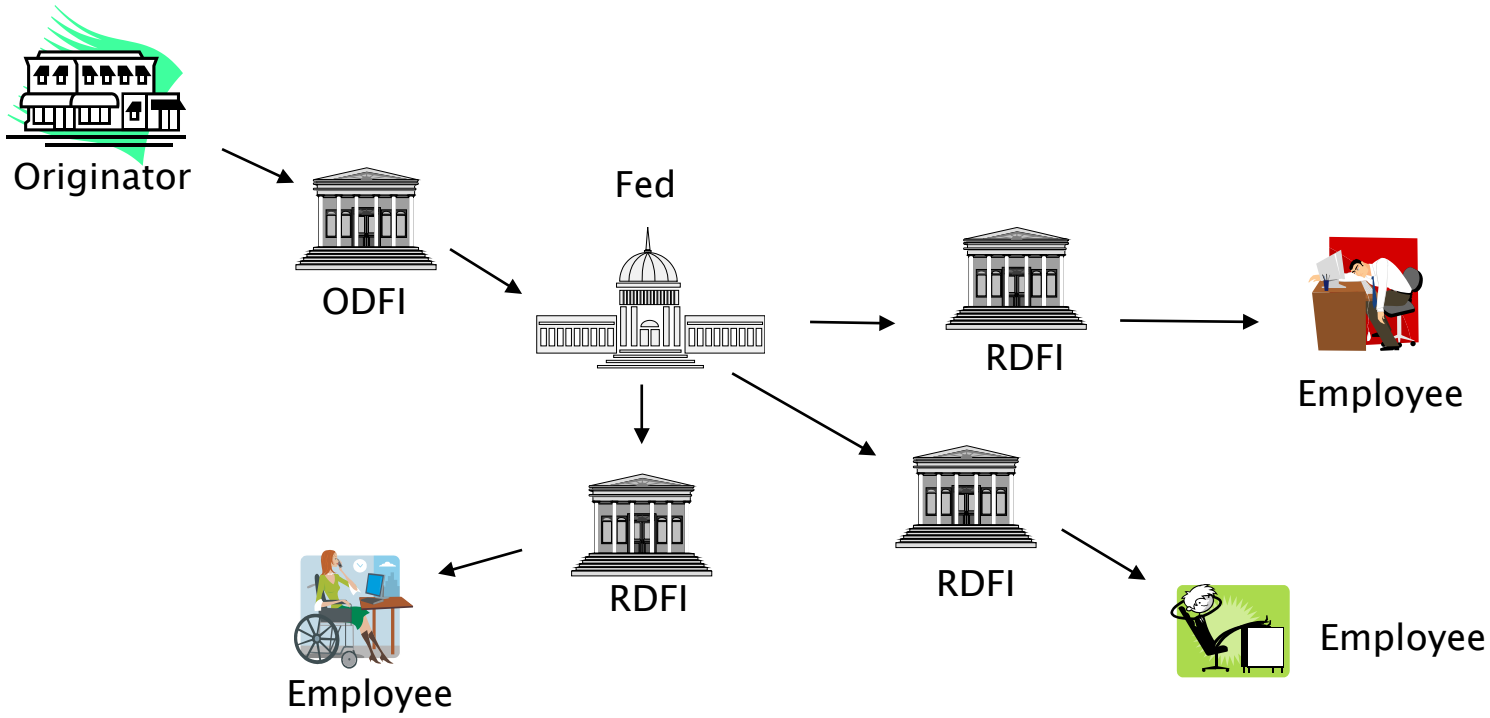
- Wire Transfers
- Automated Clearing House (ACH)
- Remote Deposit Capture (RDC)

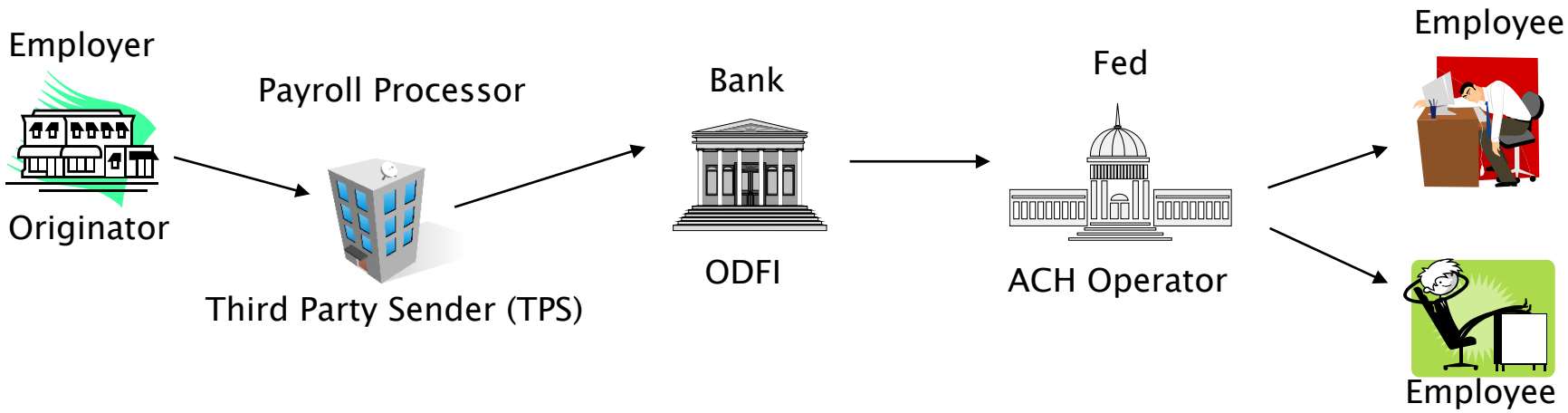
Key Terms of ACH Network

- NACHA – National Automated Clearing House Association
- ODFI – Originating Depository Financial Institution
- RDFI – Receiving Depository Financial Institution
- TPS – Third-Party Sender
- TPSP – Third-Party Service Provider

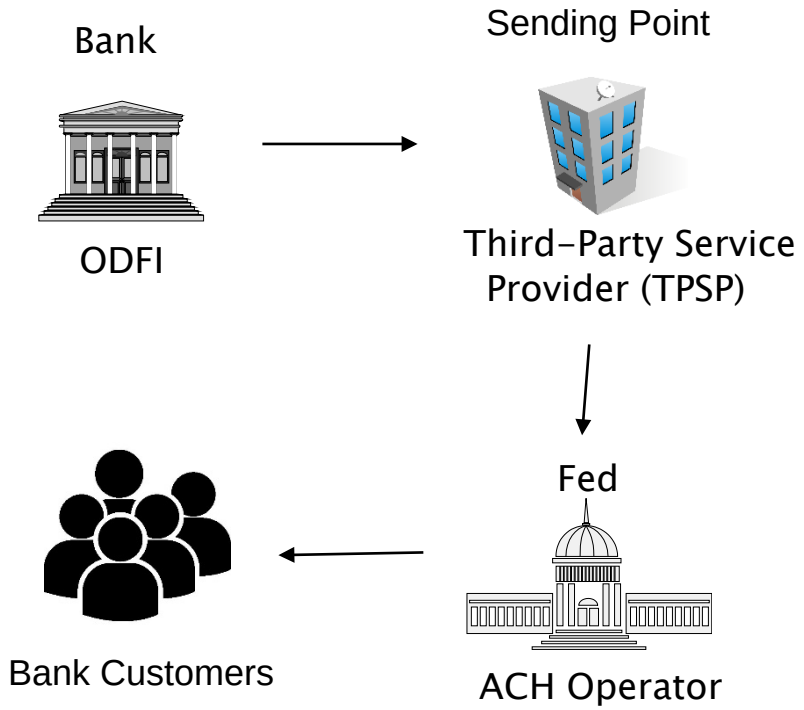
Automated Clearing House (ACH)

The Players





ACH Third-Party Service Providers (TPSP)	ACH Third-Party Senders (TPS)
Originates ACH on behalf of **an FI's** customer	Originates ACH on behalf of **their** customers
ACH Origination agreement is with **the FI** customer	ACH agreement **with TPS, not** their customer
ACH settlement account: **the FI customer's account**	ACH settlement account: **TPS' account**
Separate stand-alone agreement between FI and the (TPSP) recommended	



ODFI Controls

- Prevention of unauthorized ACH files:
  - Website Access Controls
    - Multi-factor authentication
    - Business Banking Software
  - Application software access controls
    - Issued, unique User IDs/ passwords or PINs and/or
    - ACH “switch” in Business Banking software and/or
  - Independent verification of files before release
  - Behavior Modeling of Customers (Anomaly Software)

ACH – Common Findings

- Incorrect ACH exposure limit established on the system
- ACH Risk Assessment not updated annually and/or reported to a Board/Committee
- Terminated Originator Database is not reviewed by Management as part of the onboarding or initial due diligence performed on third party senders and Originators
- Fraud controls are weak. Most financial institutions have preventive or detective controls in place but not both
- Application specific:
  - Inappropriate users with privileged access
  - A review of users' access is not performed
  - A review of administrative activity or pertinent activity is not reviewed
  - Non-immediate online banking profile closure: A customer can close their bank account, but still has access to their eBanking profile, where they can originate an ACH file, causing a loss to the bank
- Open discussion on other findings

Course Agenda

- Wire Transfers
- Automated Clearing House (ACH)
- Remote Deposit Capture (RDC)

Overview of Remote Deposit Capture

- What?

Overview of Remote Deposit Capture

- Who?
  - Commercial
    - High volume of checks for processing
    - Examples of common commercial entities using RDC
      - Property management companies, manufacturing companies, logistics companies, doctors, lawyers, etc.
  - Consumer
    - Lower volume of checks for processing

Overview of Remote Deposit Capture

- When?
  - Anytime a check needs to be cashed

- Where/How?
  - It’s remote!
  - Scanning equipment located at a company’s office
  - Mobile app on a smartphone

Overview of Remote Deposit Capture

- Why?
  - Benefits to Customer
    - Convenience – Can process anytime from anywhere. No trips to the Bank!
    - Availability of funds
  - Benefits to Financial Institution
    - Fee income
    - Increase depth of customer relationships
    - Reduced processing costs

Origination Activities – Control Points

- Approval
  - Authority to approve the customer for RDC services determined by policy
- Contract or Agreement
  - All RDC customers should have a contract or agreement on file for the RDC services
- System Setup
  - Customer setup should be reviewed for completeness and accuracy
  - Review should include per-deposit and per-day limits
- Equipment
  - Depends on contractual requirements for purchase of equipment (commercial customers)
  - If purchased or leased through FI, appropriate controls over equipment inventory should be maintained

Processing Activities – Control Points

- Image Acceptance – Control Point
  - RDC software or Institution's manual processes should detect the following:
    - Duplicates
    - Modified Images or Modified Originals
    - Piggyback Items
    - Foreign Items
    - Cross-Channel Deposits
  - Any exceptions based on system or manual detection processes should be reviewed and decisioned in a timely manner.

Processing Activities – Control Points

- Limit Monitoring – Control Point
  - Can be either systematic or manual
  - RDC software may prevent customer from submitting deposit if it is over the limits
  - Any exceptions to the per-deposit or per-day limits should be approved in accordance with policy
  - Appropriate file maintenance controls should exist over temporary limit increases and permanent limit increases

Processing Activities

- Balancing – Control Point
  - Use of multi-factor authentication (MFA) technology
- File Transmission – Control Point
  - Complete and accurate upload on the appropriate server for pick up by the core processor
  - Appropriate system access controls should exist
- Posting – Control Point
  - Non-post items should be reviewed and resolved in a timely manner

Other Risk and Control Considerations

- Monitoring
  - Annual Evaluations
  - Limit Review
  - Site Visit for Compliance Requirements (Disclosures)
- Vendor Due Diligence
  - RDC vendor should be included in vendor management program, and evaluation of the vendor should follow the requirements of the program
- Business Continuity Planning
  - FI should consider RDC service in its BCP plan

Remote Deposit Capture – Common Findings

- Periodic or annual reviews not completed timely or adequately
- Exposure limits that are established are “soft” exposure limits
- Inadequate monitoring or controls over processing of exceptions
- Inadequate policy or procedures
- Open discussion on other findings

Thank you.

For more information, contact:
Daniel Panduro
Daniel.Panduro@crowe.com