Crowe

Smart decisions. Lasting value. ™

P2P Payment Channels –
Trends, Risks, and Best Practices

Jordan Diamond and Laura Ernzen

Presenters

Jordan Diamond
Senior Manager, Financial Services
+1 216 509 1019
Jordan.diamond@crowe.com

Laura Ernzen
Manager, Financial Services
+1 615 360 5554
Laura.ernzen@crowe.com

Topics

1. **Payment Landscape and Evolving Trends: Channels, Timeline, and Compliance Considerations**

2. **Management Oversights: Risk, Controls and Fraud Prevention**

3. **Auditing Payment Systems: Summary, Best Practices and Key Areas of Focus**

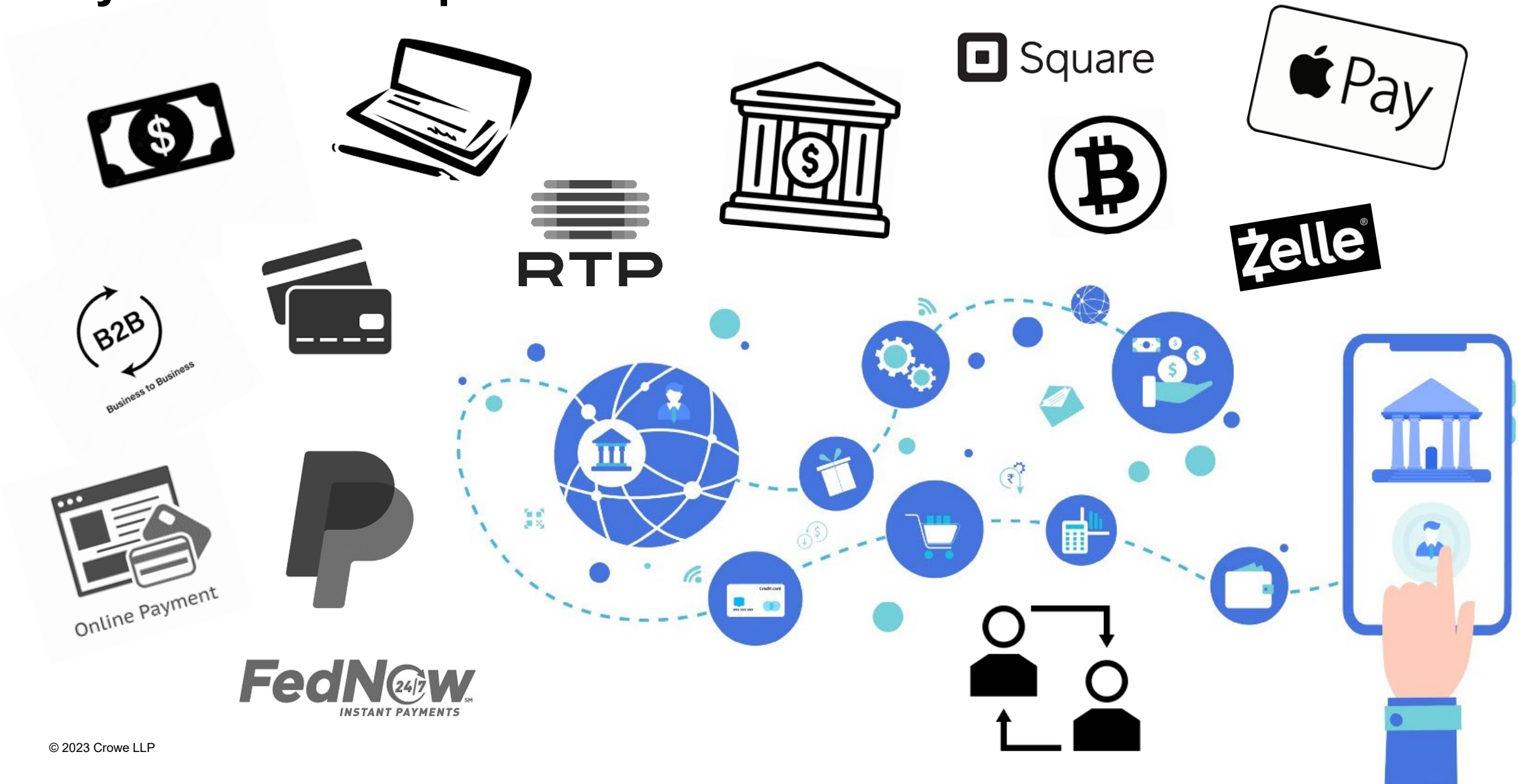
Payment Landscape and Evolving Trends

Polling Question #1

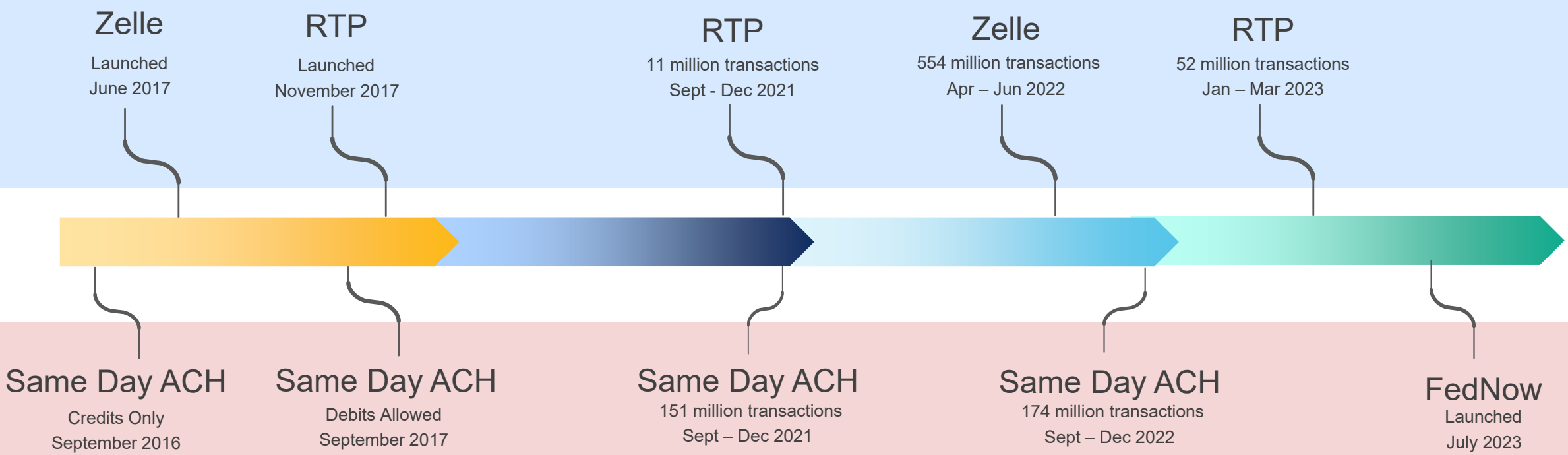
Is your organization considering Real Time Payments and/or FedNow as an offering?

a. Yes to Real Time Payments (The Clearing House)
b. Yes to FedNow
c. Yes to Both
d. We've begun having discussions, but not at this time
e. Not at this time

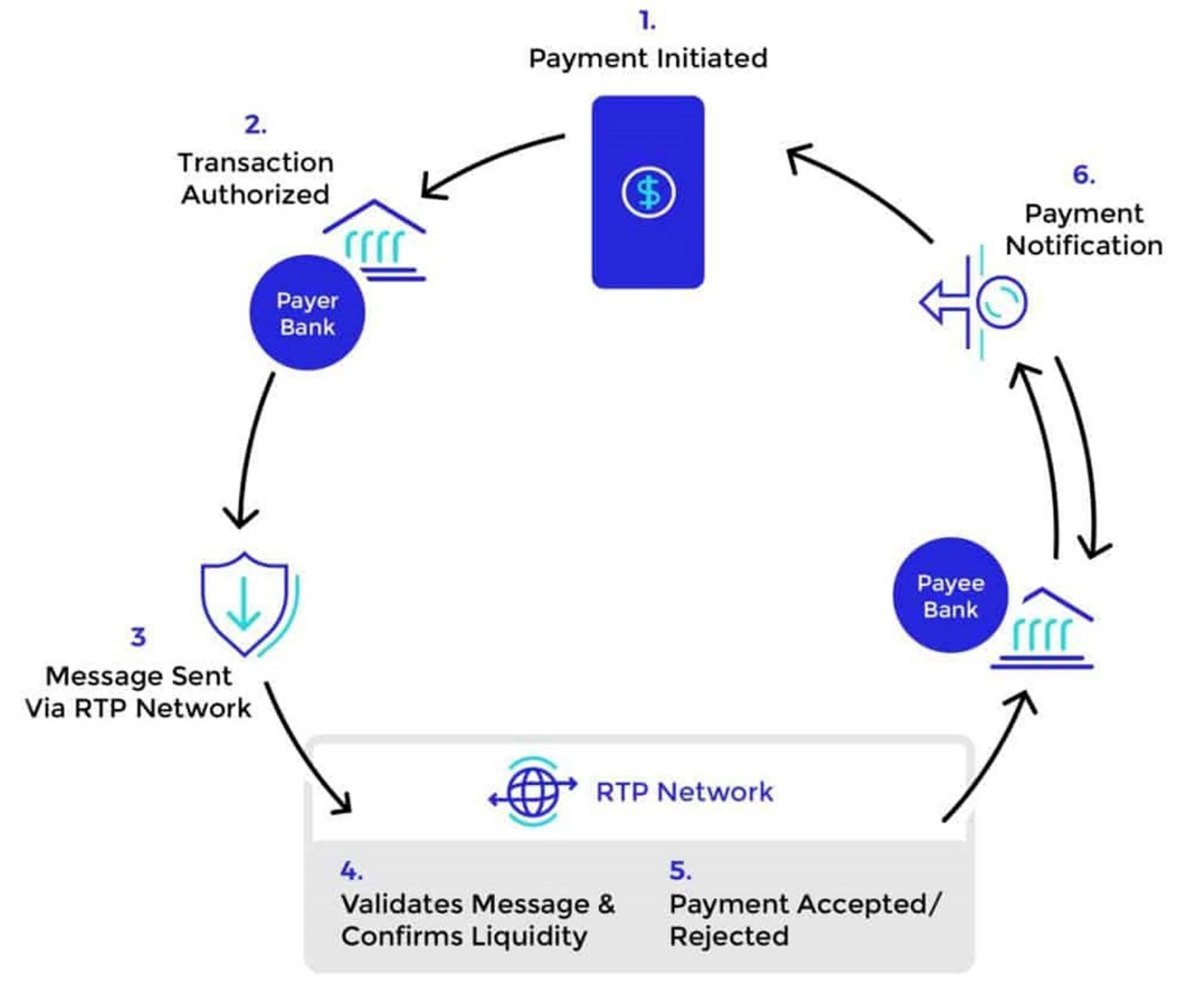
Payment Landscape and Trends



Payment Timeline



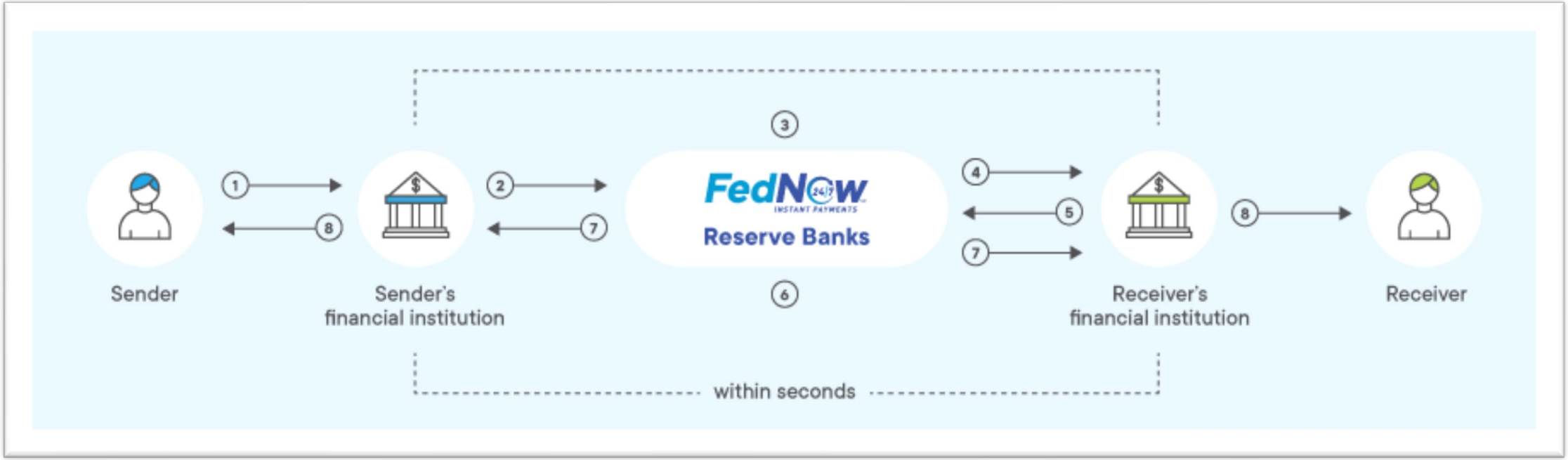
RTP



Key Attributes

- Provided by **The Clearing House**
- Instant availability and payment confirmation.
- Strictly “credit push”
- Utilized by a variety of organizations ranging from community-based to large sized institutions

FedNow



Key Attributes

- Launched in July 2023
- First phase is A2A and BillPay
- Send/receive money in seconds, 24/7
- Funds settle in real time, no interbank obligations
- Payment message sent to FedNow, instantly validated, and passes along to receiving bank for acceptance through FedNow network

Polling Question #2

Do any of your Electronic Payments Systems have integration into third parties (multiple choice)?

a. Not at this time
b. Yes, through Zelle
c. Yes, through Other
d. Unknown

Regulation E – Possible Coverage Expansion

Fraud

Someone gained **unauthorized** access to your money.

EXAMPLE

Someone gained access to your bank account without your permission. You never authorized or were involved in the transaction.

CAN YOU GET YOUR MONEY BACK?

Because you **did not authorize a payment**, you are typically able to get your money back.

Scam

You authorized a payment, but didn't receive what was expected.

EXAMPLE

You used Zelle® to send money to someone on the Internet for concert tickets, but you never received the tickets.

CAN YOU GET YOUR MONEY BACK?

Because you **authorized the payment**, you may not be able to get your money back.

Polling Question #3

Are you able to get your money back in the event of a scam?

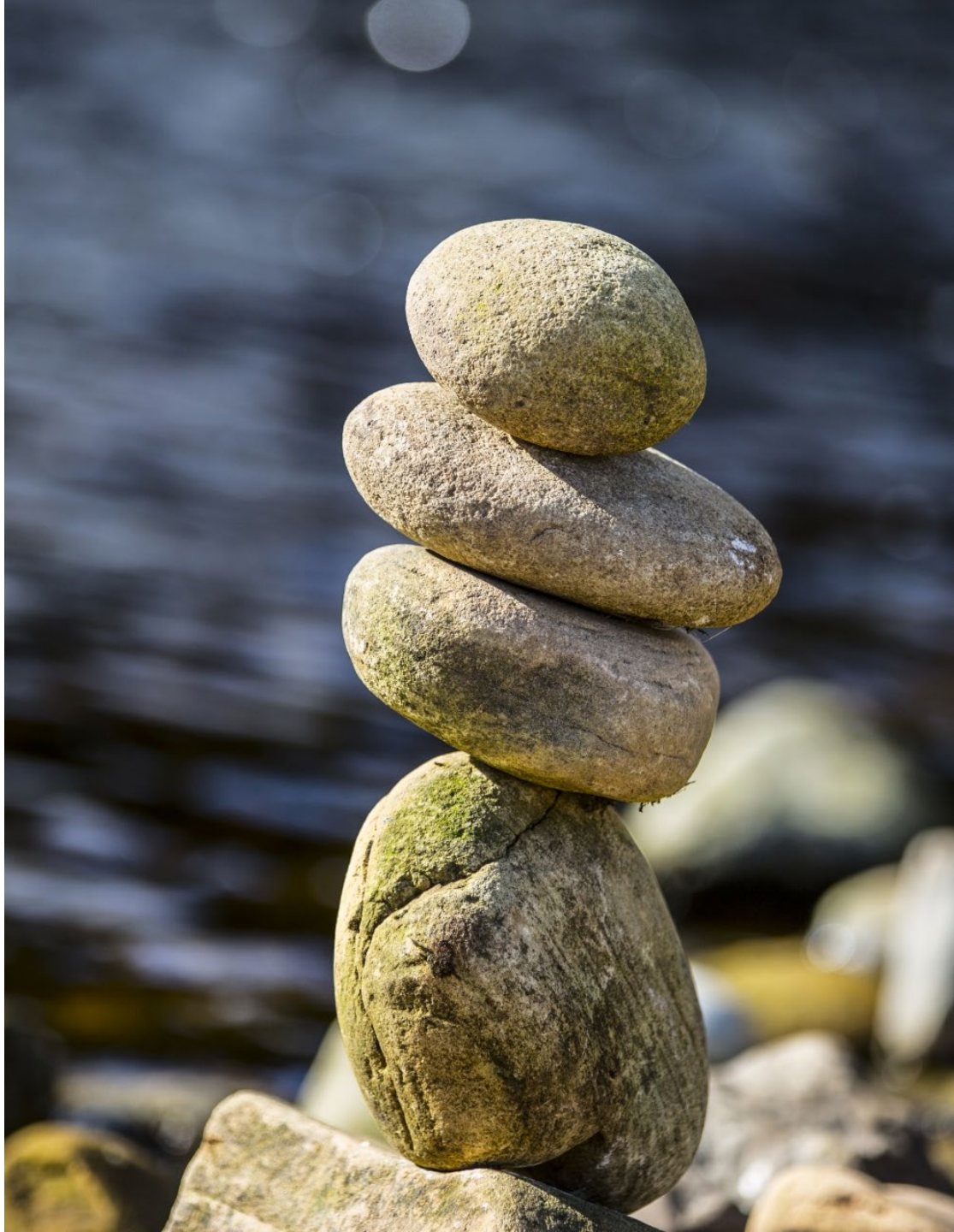
a. Yes, I authorized the payment
b. No, I authorized the payment
c. What scam?
d. No, I did not authorize the payment

Management Oversight

Finding the Balance

- Moving forward with emerging technology while balancing speed to market and risk.

- New payment features or channels need the same robust scrutiny you'd apply to a new product/service or line of business



Payment Risks and Controls

Key Questions

Determining Inherent Risk

- What is the Inherent Risk or Risk without controls?
- How likely is a risk to exist? How significant is its impact?
- Have you documented your analysis?
- What considerations were included? i.e volume of activities, complexity of operations, capability of the department?

Measuring Effectiveness of Controls

- What are the controls and governance mitigating risk?
- How effective is the design control, how well are they operating?
- Are your controls strong, satisfactory, or weak
- What are the quality of policies providing guidance?
- Are the procedures detailed, current, complete?

Risk Considerations

Systems and Controls	Credit Risk	High Risk Activities	Compliance Risk	Transactional/ Operational (Incl. Fraud) Risk	Third Party Risk	Information Technology Risk	Strategic Risk	Reputation Risk	Overall Inherent Risk
Moderate	Moderate	Low	Moderate	High	Moderate	High	Moderate	Moderate	Moderate

Credit Risk - *The risk of loss associated with a borrower or counterparty default (failure to meet obligations in accordance with agreed upon terms).*

Operational Risk -*The risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events.*

Compliance Risk - *The risk resulting from the failure to comply with laws (legislation, regulation, and rules) and regulatory guidance and the failure to appropriately address associated impact, including to clients.*

Financial Risk *- The risk of losing money on an investment or business decisions which may impact the bank's ability to meet its obligations or pay its debts.*

Reputation Risk - *The risk arising from the potential that negative stakeholder opinion or negative publicity regarding the Bank's business practices, whether true or not, will adversely impact current or projected financial conditions and cause a decline in the client base, or result in costly litigation. Stakeholders include employees, clients, regulators, elected officials, social media posters, advocacy groups and media organizations*

Strategic Risk - *The risk to earnings, capital or liquidity arising from adverse business decisions, improper implementation of strategic initiatives or inadequate response to changes in the external operating environment.*

Fraud Prevention

- Share Account Searching
- Multi-factor Authentication
- Member and Business Onboarding & Fraud Alerting
- Fraud Monitoring and Reporting

Auditing Payment Systems

Payment Processing Summary

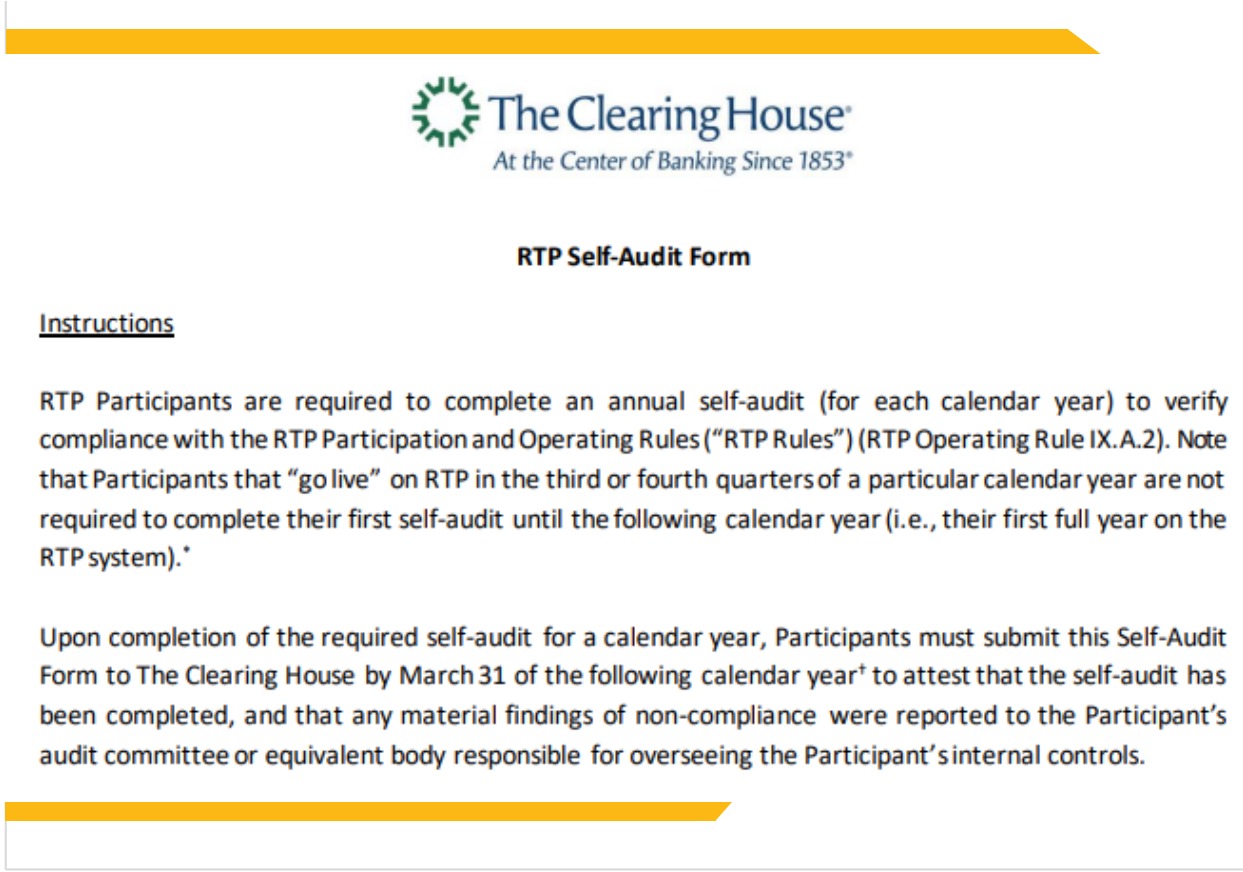
Payment Type	Technology	Owner / Operator(s)	Regulation	Audit Type	Platform Daily Limit	Payment Direction	Foreign Payments Allowed?	Funds Availability	Settlement
Real Time Payments	Rail / Network	The Clearing House LLC	RTP Operating Rules	Annual Compliance Audit	$1,000,000	Credit Only *Supports a request for payment	No	Instant or Near-Instant	Daily
FedNow	Rail / Network	The Federal Reserve	TBD	TBD	$500,000	Credit Only *Supports a request for payment	No	Instant	Immediate
ACH	Rail / Network	The Federal Reserve & EPN	NACHA Operating Rules	Annual Compliance Audit	$1,000,000	Credit & Debit	Yes	Same Day	Daily
Zelle	Application / Software	Early Warning Services LLC	Based on Underlying Payment Rail	Based on Underlying Payment Rail	Based on Underlying Payment Rail	Credit Only *Supports a request for payment	No	Based on Underlying Payment Rail	Based on Underlying Payment Rail

Polling Question #4

Has your organization given audit scope consideration to payment applications such as Zelle, RTP, FedNow?

a. Yes
b. No
c. Not sure

Audit Timing Requirements – RTP and NACHA



The Clearing House
At the Center of Banking Since 1853

RTP Self-Audit Form

Instructions

RTP Participants are required to complete an annual self-audit (for each calendar year) to verify compliance with the RTP Participation and Operating Rules ("RTP Rules") (RTP Operating Rule IX.A.2). Note that Participants that "go live" on RTP in the third or fourth quarters of a particular calendar year are not required to complete their first self-audit until the following calendar year (i.e., their first full year on the RTP system).*

Upon completion of the required self-audit for a calendar year, Participants must submit this Self-Audit Form to The Clearing House by March 31 of the following calendar year† to attest that the self-audit has been completed, and that any material findings of non-compliance were reported to the Participant's audit committee or equivalent body responsible for overseeing the Participant's internal controls.

Nacha

The Nacha Operating Rules and Guidelines require that all participating depository financial institutions, third-party senders and third-party service providers that provide ACH services to the RDFI or ODFI, conduct an annual ACH audit by December 31 of each year (ACH Rules, Article 1).

Real Time Payment Scope and Common Findings

Summary of Key Rules Topics to Consider for RTP Audit:

1. 24/7 Operation
2. Message Persona
3. Payment Status/Message Information
4. No Correspondents
5. No Fee Netting
6. No Searching for Accounts
7. No Foreign Payments
8. Transaction Limit
9. Receiver Name
10. Directory Service
11. Payment Message Response
12. Payment Response Time
13. Payment Message Acceptance
14. Funds Availability
15. Funding Obligation
16. Funding
17. Non-Funding Participants
18. Non-Payment Messages
19. Fraud Reporting and Acting on Alerts
20. Controlled Access
21. Multi-Factor Authentication
22. Fraud/Risk Monitoring
23. Respond to Reports of Abuse
24. OFAC
25. Errors/Unauthorized Payments (Cooperation)
26. RFR Response
27. RFP Due Diligence
28. RFP Monitoring
29. RFP Investigation
30. RFP Corrective Action
31. PSP Customers

Common findings:

- Transaction limits are not set up properly
- Fees are not separated for line items (i.e., not netted together with payment)
- System access to RTP systems
- Agreements do not protect the Bank in the event of suspected misuse of RTP systems
- Policies and procedures are not reflective of control environment

ISO Compliance – Best Practice (FedNow)

e. Value Messages

Value messages initiate a funds transfer and are processed and settled through the FedNow Service via the Master Account of the Participant or its Correspondent. Value messages include Customer Credit Transfer (pacs.008), payment return (pacs.004) and Liquidity Management Transfer (pacs.009).

ISO 20022 Message	Used by	Message Functionality
pacs.008 Customer Credit Transfer	Participants	Instructs the FedNow Service about a single instant payment where either the initial sender or final receiver, or both, are not FIs.
pacs.004 Payment return	Participants	Return of previously received funds.
pacs.009 Liquidity Management Transfer	Participants	Instructs a single payment where both sender and receiver are financial institutions.

NACHA Scope and Common Findings

o General Self-Audit	o RDFI Self-Audit
o General - All Institutions	o RDFI - All Institutions
o ODFI Self-Audit	o RDFI - Availability and Posting - All Institutions
o ODFI - Agreements - All Institutions	o RDFI - Dishonored Returns
o ODFI - All Institutions	o RDFI - General Returns - All Institutions
o ODFI - Debit Auth Request	o RDFI - NOC
o ODFI - Dishonored Returns	o RDFI - Permissible Returns
o ODFI - Exposure Limits - All Institutions	o RDFI - Prenotifications
o ODFI - NOC	o RDFI - RCK Returns
o ODFI - Originator Identity - All Institutions	o RDFI - Special Returns
o ODFI - Permissible Returns	o RDFI - Statement Content - All Institutions
	o RDFI - Stop Payments
o ODFI - Prenotifications - All Institutions	o RDFI - UCC4A - All Institutions
o ODFI - Registration - All Institutions	o RDFI - Unauthorized Returns
o ODFI - Reversing Entries	
o ODFI - Same-Day ACH Origination	
o ODFI - UCC4A - All Institutions	

Common Findings:

- Returns are not processed in accordance with NACHA rules (timeliness of return and/or return code)
- R03 vs R04
- Written Statement of Unauthorized Debits – missing items on form
- Originator exposure limit review
- Policies and procedures are not reflective of current environment

Thank You