



Financial Horizons: Navigating Trends in Healthcare Finance

Samantha Werner | January 26



CommerceHealthcare®

Today

- The Landscape
- Liquidity Management
- Reconciliation Strategies
- Fraud Prevention in Healthcare
- Payments Automation
- Summary / Q&A

Today's Landscape



Healthcare Complexity



Mergers & Acquisitions



Evolving Models for Reimbursement



Complex and Non-standard Payers



Multiple Electronic Systems



Fees Incurred with Payments

Organizations are looking for **Automation**

Challenges result in manual, costly, fragmented and **inefficient processes**, such as:



Management of payment receipt, posting, and reconciliation



Payer complexity, PLBs, etc.



Payer credit card processing fees upwards of 3-4%



How to make images intelligent?

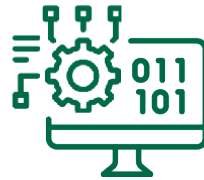
Treasury Management Trends

Key Trends Influencing Treasury Management in 2024 & Beyond



Rapidly Changing Rate Environment

- Rates have elevated historically quick
- Deposits remain at all-time highs
- Focusing on cash conversion cycle crucial



Embedded Product Innovation

- API's and other plugins allow organizations to manage payments and reconciliation directly from their ERP/TMS



Payment Rail Modernization

- RTP's are on the horizon while same day ACH's and virtual cards are still growing significantly



Acceleration of Digitization & Automation

- RPA & OCR across Payables & Receivables
- AI & ML applied to growing data sets
- Digitally Driven Customer Experience Expectations Impacting more business models

Liquidity Management



Fed Rate Changes 2022 thru 2023

FOMC Meeting Date	Rate Change (bps)	Federal Funds Rate
July 26, 2023	+25	5.25% to 5.50%
May 3, 2023	+25	5.00% to 5.25%
March 22, 2023	+25	4.75% to 5.00%
Feb 1, 2023	+25	4.50% to 4.75%
Dec 14, 2022	+50	4.25% to 4.50%
Nov 2, 2022	+75	3.75% to 4.00%
Sept 21, 2022	+75	3.00% to 3.25%
July 27, 2022	+75	2.25% to 2.50%
June 16, 2022	+75	1.50% to 1.75%
May 5, 2022	+50	0.75% to 1.00%
March 17, 2022	+25	0.25% to 0.50%

Treasury Yields

2-Year Treasury



10-Year Treasury



Rate Predictions for 2024



CNBC

<https://www.cnbc.com> › 2023/12/13 › fed-interest-rate-... ⋮

Fed holds rates steady, indicates three cuts coming in 2024

Dec 13, 2023 — Three more reductions in 2026 would take the fed funds **rate down to between 2%-2.25%**, close to the long-run outlook, though there was ...



Reuters

<https://www.reuters.com> › markets › fed-likely-hold-rat... ⋮

With rate hikes likely done, Fed turns to timing of cuts

Dec 13, 2023 — Indeed, the shift in outlook was stark, with 17 of **19 Fed policymakers seeing rates lower by the end of 2024**, and none seeing them higher. A ...



money.com

<https://money.com> › ... › Federal Reserve ⋮

When Will the Fed Cut Interest Rates? Predictions for 2024

Dec 26, 2023 — Fed interest rate cuts could begin in **early 2024**, according to some experts. Other experts predict that cuts won't start until late 2024.

Liquidity Topics to Consider



Impact of high rates
on borrowing

Fixed vs floating rates



Impact of rates on
investing

Short vs Long Term Options



Investment Policy
Concerns

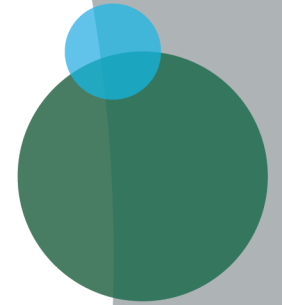
Yield vs Risk Tolerance



Impact of AR Days
and AP Days

Cash flow dollars

Reconciliation Strategies



Questions to Ask



- How often do you reconcile your bank accounts?
- Do you reconcile your cash received to your cash posted?
- How manual is your current reconciliation process?
- Recon impact to month-end close timing?

Challenges with Traditional Recon Processes



Time
Consuming



Inaccurate
Reporting



Lack of
Standardization



High Risk &
Compliance
Issues



Lack of
Visibility

Benefits of Improved Account Reconciliation



Improved accuracy & cash flow



Fraud prevention



Compliance



Better decision making



Data integration



AI-powered matching



End to end reconciliation management



Exception handling

Tools for Reconciliation

ERP Capabilities

- Import/export options
- BAI2

Third Party Systems

- Trintech
- Crowe
- Others?

Fraud Prevention


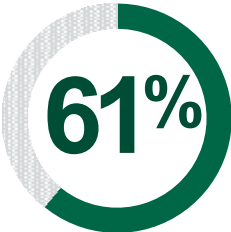





2023 AFP Fraud Study | Key Insights¹



¹ 2023 AFP® Payments Fraud and Control Report

Cybersecurity Will Consume Major Leadership Attention

Ransomware	Payment Fraud	Healthcare Vulnerabilities	Leadership Confidence
			
67% of healthcare organizations impacted 33% more than once	of fraud attacks target Accounts Payable 13% target Treasury	Phishing, outdated software patches, unsupported software, poorly configured Internet access	61% of leadership lacks confidence in organizational ability to combat ransomware
\$21 BILLION Downtime cost to industry	Business email compromise is the root cause	Growing problem with attacks through third-party apps and APIs to central systems	

Ransomware Attacks



Ransomware is most often associated with malware designed to cripple businesses by either making their computer systems unusable or by holding proprietary, sensitive and often private data hostage until the target pays money or “ransom.”



Governments worldwide saw a 1,885% increase in ransomware attacks, and the health care industry faced a 755% increase in 2021 attacks¹



Ransomware attacks in North America rose by 158% between 2019 and 2020, compared to a global increase of 62%²



The FBI received almost 2,500 complaints about ransomware in 2020, a 20% increase from the previous year²

¹ 2022 SonicWall Cyber Threat Report

² <https://www.pymnts.com/news/security-and-risk/2021/treasury-reports-590m-in-suspected-ransomware-payments>

Business Email Compromise



Executive Email Compromise

- 1 High level email account is compromised or spoofed
- 2 Email account used to send fraudulent payment instructions to 2nd employee or financial institution; "Urgent & Confidential"
- 3 Funds transferred to account controlled by criminal



Employee Email Compromise

- 1 Low to mid-level employee email is compromised or spoofed
- 2 Fraudulent invoices sent from employee email account to vendors
- 3 Funds transferred to account controlled by criminal



Vendor Impersonation Fraud

- 1 Criminal impersonates legit vendor via email, phone, fax, mail
- 2 Requests update to vendor account information; account and routing number changed to direct future payments to fraudulent account
- 3 When the next legit invoice is received, funds are transferred to account controlled by criminal

Vendor Impersonation is on the Rise



Vendor Impersonation occurs when a business receives an unsolicited request, purportedly from a valid vendor, to update the payment information for that vendor, when in fact it is a fraudster impersonating the vendor.



Monitoring

Fraudster monitors a business for publicly available vendor information using the same tactics as BEC



Posturing

Fraudster contacts the business by posing as the legitimate vendor to request updates or changes to the payment information



Execution

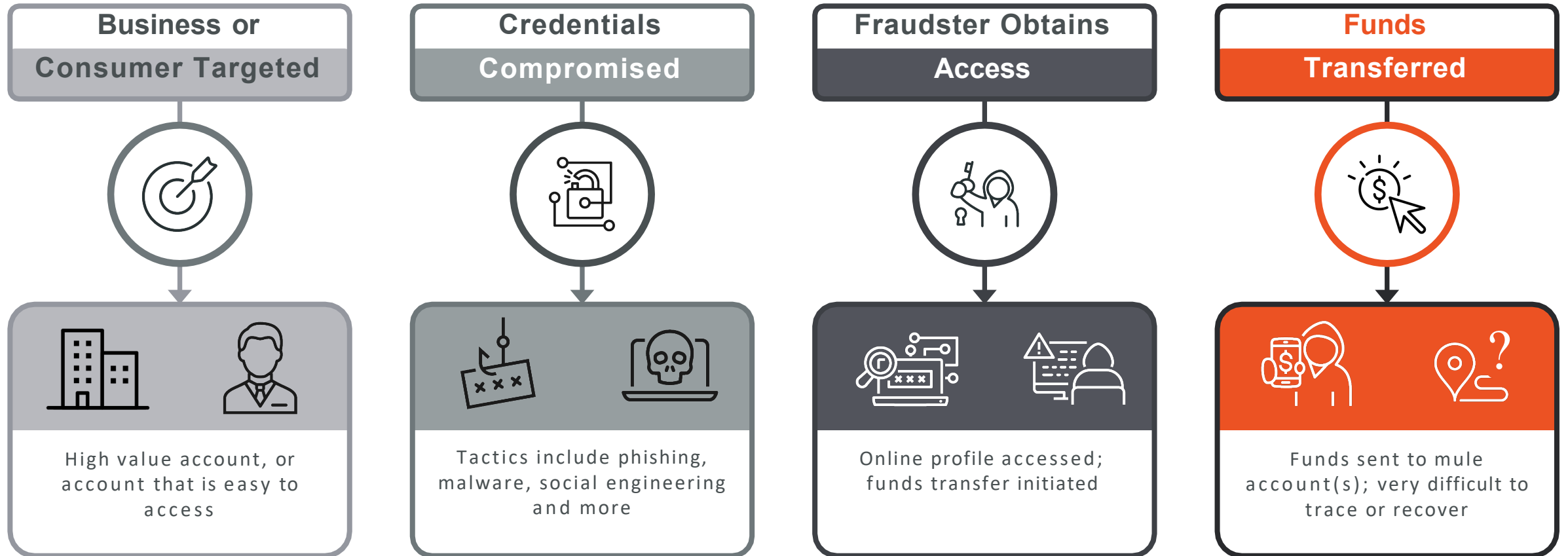
Using fraudulent instructions, funds are transferred to an account controlled by the fraudster



On the Rise

BEC fraud is becoming more sophisticated as ACH-related fraud trends upward

Account Takeover



Fraud Prevention



Fraud remains on the rise – protect you and your company from fraudulent activity by proactively following these six tips:



1 Be suspicious of unsolicited emails and phone calls



2 Establish dual control for online money movement



3 Confirm vendor payment instructions with a verified contact



4 Review transactions daily; if possible, perform daily reconciliations



5 Use available account protections like ACH Risk Manager & Positive Pay for checks



6 Inform Commerce Bank of any suspicious activity on your accounts

Business Email Compromise (BEC) is a primary source of attempted or actual payments fraud at **68% of companies***



In 2021, 71% of organizations were targets of **payment scams** with **checks and wire transfers** the payment methods **most impacted by fraud***

* Source: The 2021 AFP® Payments Fraud and Control Survey

What To Do If You Are A Victim



Four recommended follow up actions in the event of suspected fraud:

1



Notify your financial institution

2



Businesses should notify their IT Department

3



Contact your local FBI Field Office

4



File a complaint with [ic3.gov](https://www.ic3.gov)

Best Practices for Defense

1



Know your business partners

Vet prospective partners

2



Maintain internal controls

Separation of duties and ongoing cross training

3



Educate and train employees

- Keep employees informed of the forms of BEC and phishing attempts
- Look carefully for small changes in email addresses that mimic legitimate emails (.co vs. .com, abc-company.com vs. abc_company.com, or hijkl.com vs. hljkl.com.) If you receive an email that looks suspicious, forward it to IT for review.
- Independently authenticate changes in payment instructions (outside of email, using number on file)
- Be cautious of requests for secrecy, or pressure to take action quickly
- **Do not use the 'reply' option** when authenticating emails for payment requests. Use the 'forward' option and type the correct email address or select from a known address book

Best Practices for Defense

4



General Internet Security

- Try to keep computers that transact business in a **secure location**
- Use the **time-out function** when you are away from your computer that requires a password to log back in
- Sign out and close your browser after you're finished with an online application.
- Install new security patches as your operating system and internet browsers make them available
- Do not provide **nonpublic business information on social media**

5



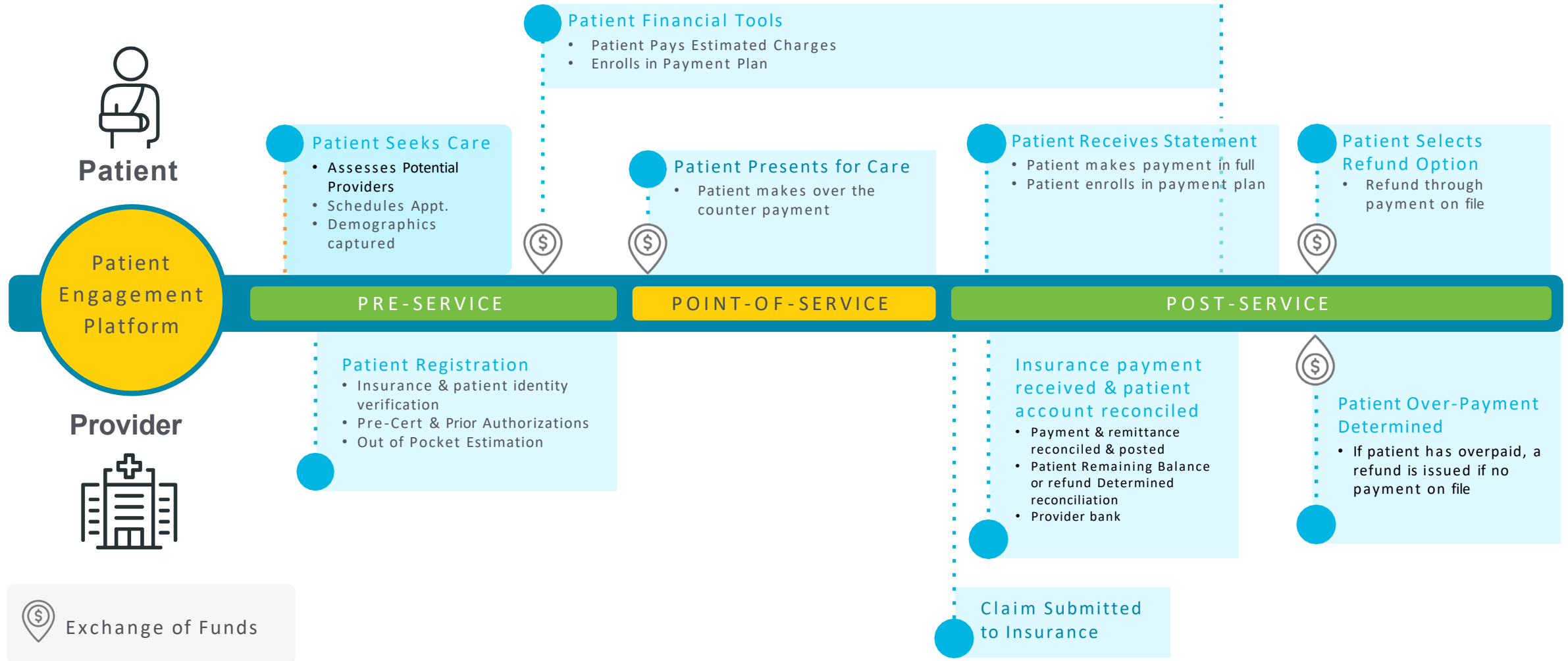
Banking Best Practices

- If possible, have a dedicated computer for online financial transactions
- Review transactions daily; if possible, do a **daily reconciliation**
- Set up transaction alerts
- Use available **account protections**

Payments Automation



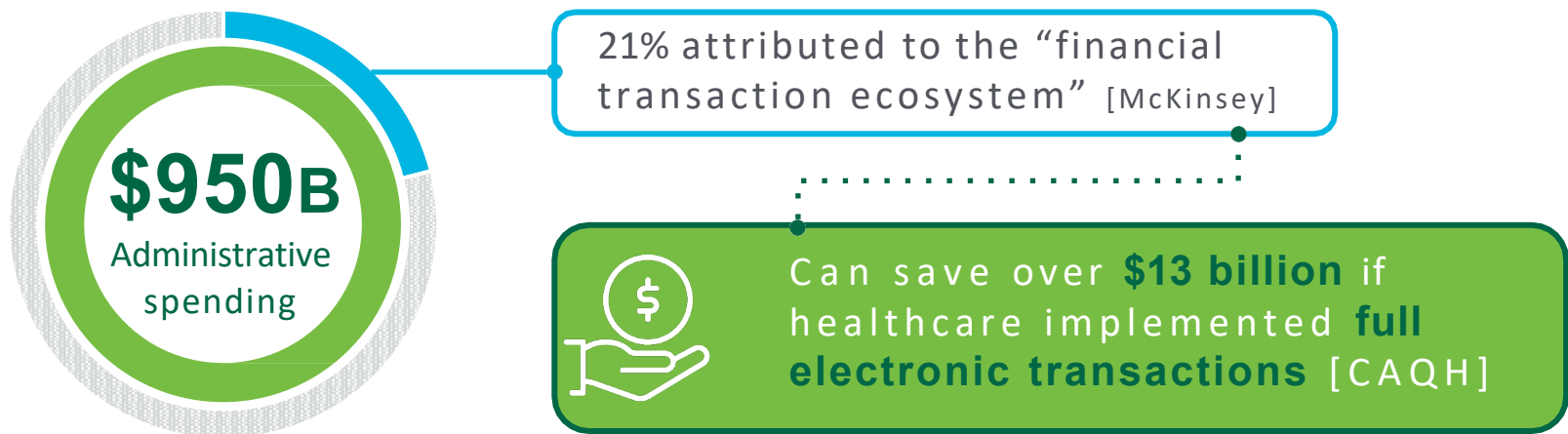
The Patient Journey



Major Advancement Opportunity for RCM/Finance Automation



Substantial Savings Potential



Three financial automation drivers:



Staffing issues



Growing data need for analytics



Widening gap between cost of automated & manual transactions

For providers whose payment or invoice processes were not automated, average DSO jumped **17%** during the pandemic

Payment Automation Questions

Accounts Receivable

- Claims & patient billing process?
- Co-Pays and pre-service payments?
- Online payment portal?
- Payment plan options?
- AR posting files?
- Payment methods accepted?

Accounts Payable

- Where do invoices come into org?
- Paper vs Image approval workflow?
- How quickly are payments made?
 - Discounts/Late fees
- Payment methods used?
- Patient refund process?

Benefits of AP Automation



Transitioning from manual to **automated accounts payable** can play a vital role in turning your **AP department** into a **profit center**.



Create
AP Process
Efficiencies



Reduce
Costs



Eliminate
Paper



Increase
Electronic
Payments



Maximize
Employee
Resources

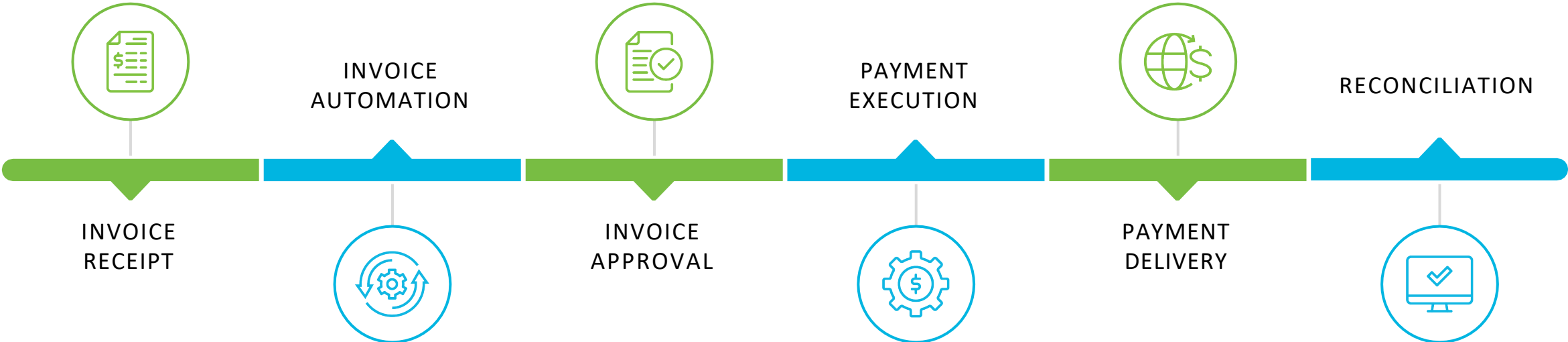


Earn Revenue
Share with AP
Card

Optimize Payables



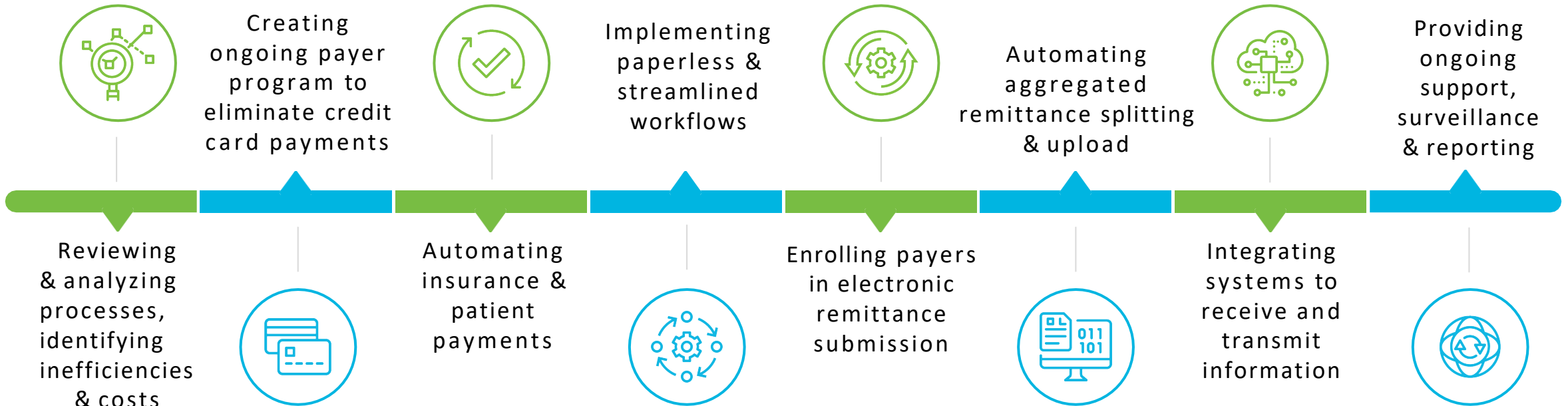
Takes care of your invoices from beginning to end by maximizing your efficiencies and replacing your manual AP processes. Invoices are received, scanned, approved, paid, and reconciled according to your rules and policies.



Optimize Receivables



Navigating revenue cycle complexities can help your organization **identify and optimize processes**, saving you **time** and **money** by:





Questions/Open Discussion

Commerce Bank is CommerceHealthcare®

➤ We don't just serve the healthcare industry. **It's our specialty.**



Partner to
**500+ hospital
systems**

in all 48
contiguous States



\$1.7 billion+ in
patient loans
funded



\$10B+
processed
annually
on Visa network



\$1B+ in
commercial loans
outstanding
and over \$2B in
healthcare credit
commitments



**ROI based
solutions**



Natural extension
of our **core
capabilities**



**National
Healthcare
team**

Patient Engagement Solutions

- Patient Financing
- Online Bill Pay
- Patient Refunds

Treasury Receivables Solutions

- Receivables Optimization
- Reconciliation Automation
- Healthcare Lockbox

Accounts Payable Solutions

- End to end payment automation
- Virtual Card Revenue Share
- Invoice Automation

Banking and Investment Services

- Credit support
- Days Cash Investment
- Institutional Trust Services



- HEALTH SERVICES FINANCING (HSF®) PATIENT LENDING
- REMITCONNECT®
- VIRTUAL CARD

Guest Presenter



Sam Werner

Senior Vice President, Treasury Market Manager

Samantha.Werner@CommerceBank.com | 816.234.2940

Samantha is Senior Vice President and Treasury Market Manager. Since joining Commerce in 2018 her primary focus is working with health systems and insurance companies. She also leads our Treasury Healthcare team who focus on large health systems with over \$250MM in net patient revenue. Samantha received her BS in Marketing from Southwest Missouri State University. She maintains her Accredited ACH Professional (AAP) certification and Certified Treasury Professional (CTP) certification. With 23 years of Treasury Management experience, Samantha offers her clients a wealth of experience in streamlining cash flow, improving efficiencies, and mitigating fraud.