

Finance Trends in Healthcare: A Focus on Fraud Mitigation & Payments Automation

Samantha Werner | April 2024



CommerceHealthcare[®]

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

Today

- Today's Landscape
- Fraud Prevention
- Payments Automation
- Summary / Q&A

Today's Landscape



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



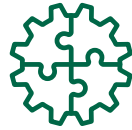
Impact of AR Days and AP Days

Cash flow dollars

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?

Another Year of Financial Recovery



Industry **progress** in 2023, but still a difficult year. **Greater labor and supply expense and patient acuity will continue to be a challenge**



Median hospital operating margin rose 2% in November, with margins varying among institutions & markets

\$64 Billion

Financial Reserves fell by \$64 billion across the board

Cash on Hand

73% of nonprofit hospitals and health systems saw "strong" levels of cash on hand



Many providers continue to contend with an imbalance between rate of growth across expenses and revenue

Technology is part of solution,
not entire solution

but

AI, automation, HER optimization, virtual care programs and remote patient monitoring are increasingly important in helping to close some care gaps

Physician Shortage
by 2034

U.S. faces an estimated shortage of between 37,800 and 124,000 primary care and specialists physicians

Another Year of Financial Recovery



Industry progress in 2023, but still a difficult year. **Greater labor and supply expense and patient acuity will continue to be a challenge**



Median hospital operating margin rose 2% in November, with margins varying among institutions & markets

\$64 Billion

Financial Reserves fell by \$64 billion across the board

Cash on Hand

73% of nonprofit hospitals and health systems saw "strong" levels of cash on hand



Many providers continue to contend with an imbalance between rate of growth across expenses and revenue

Technology is part of solution,
not entire solution

but

AI, automation, HER optimization, virtual care programs and remote patient monitoring are increasingly important in helping to close some care gaps

Physician Shortage
by 2034

U.S. faces an estimated shortage of between 37,800 and 124,000 primary care and specialists physicians

Major Advancement Opportunity for RCM/Finance Automation



Substantial Savings Potential



21% attributed to the “financial transaction ecosystem” [McKinsey]

 Can save over **\$13 billion** if healthcare implemented **full electronic transactions** [CAQH]


Three financial automation drivers:



Staffing issues



Growing data need for analytics



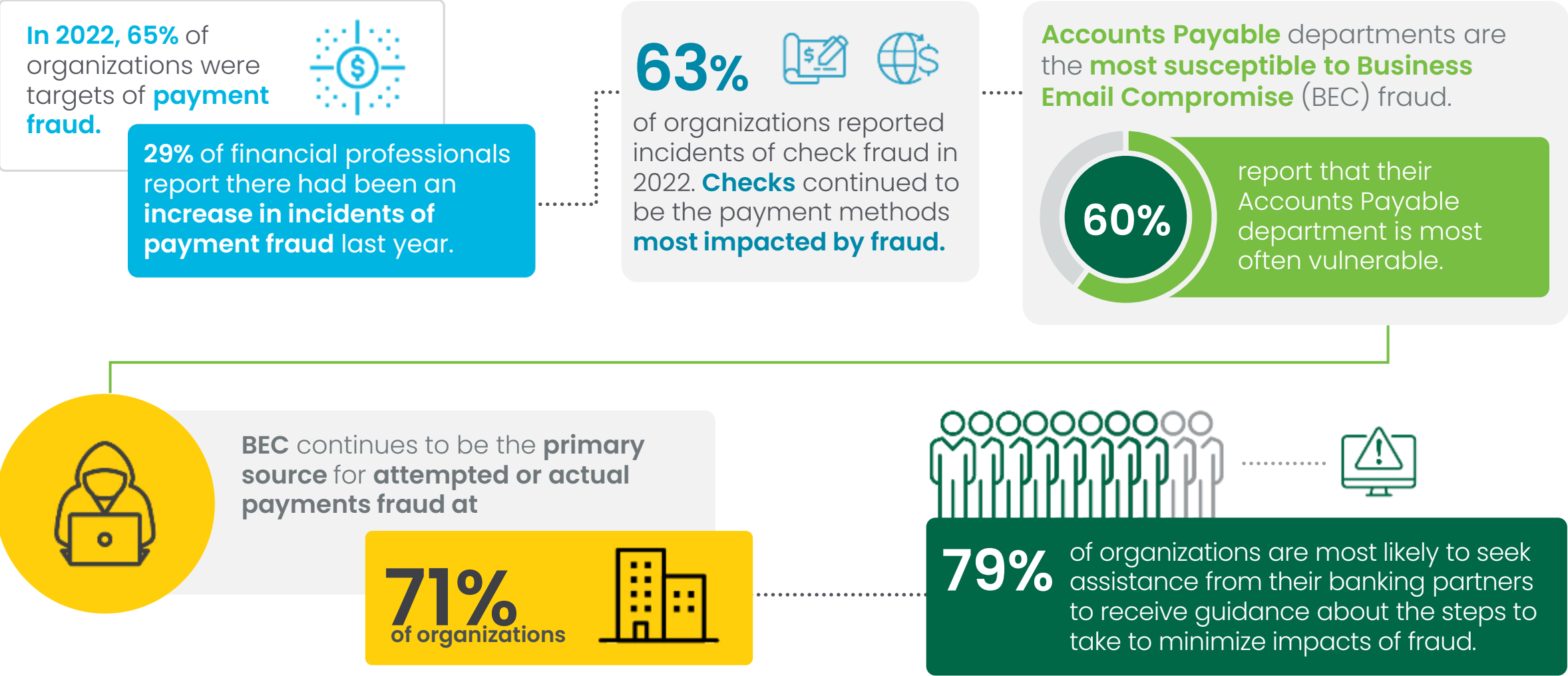
Widening gap between cost of automated & manual transactions

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

Fraud Prevention



2023 AFP Fraud Study | Key Insights¹



¹ 2023 AFP® Payments Fraud and Control Report

Cybersecurity Will Consume Major Leadership Attention

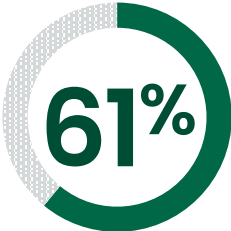
Ransomware



67% of healthcare organizations impacted
33% more than once

\$21 BILLION
Downtime cost to industry

Payment Fraud



of fraud attacks target **Accounts Payable**
13% target **Treasury**

Business email compromise **is the root cause**

Healthcare Vulnerabilities



Phishing, outdated software patches, unsupported software, poorly configured Internet access

Growing problem with attacks through third-party apps and APIs to central systems

Leadership Confidence



61% of leadership lacks confidence in organizational ability to combat **ransomware**



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 year**²

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

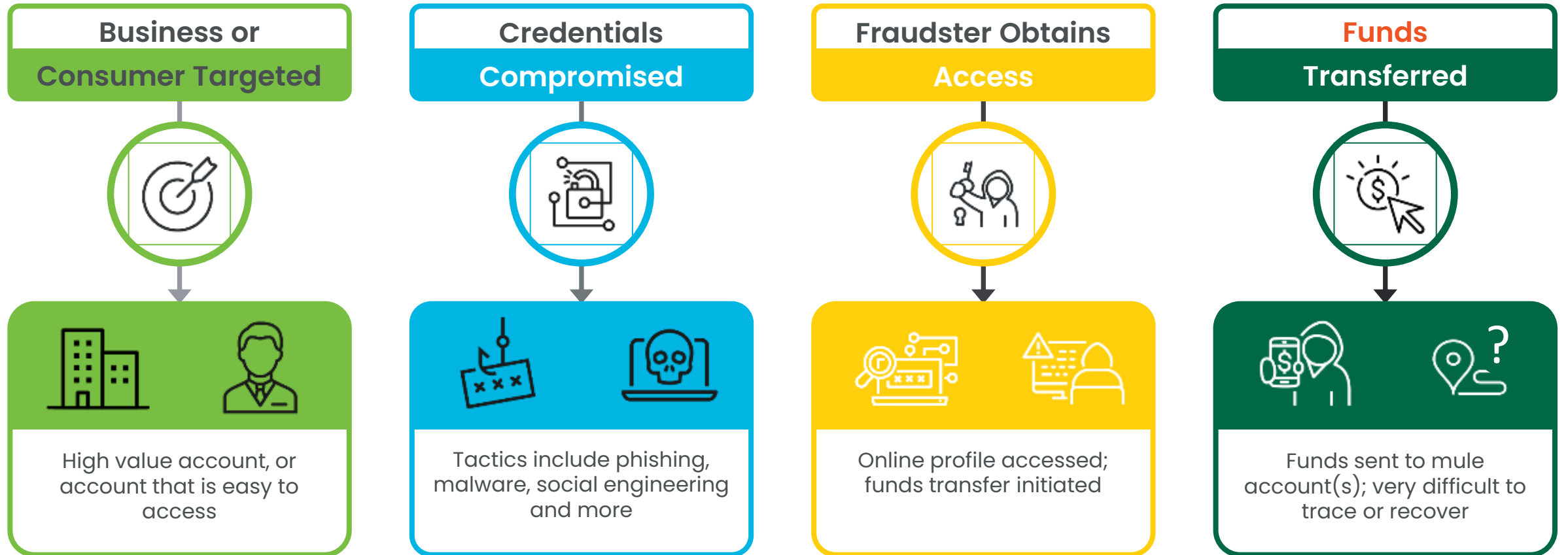
Using fraudulent instructions, funds are transferred to an account controlled by the fraudster



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

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



Accounts Payable Questions

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

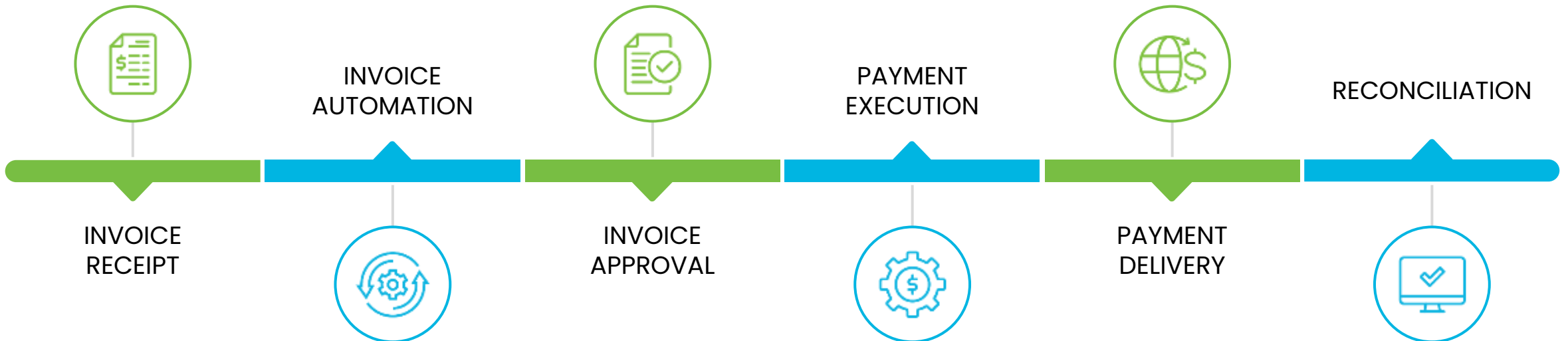


Earn Revenue
Share with
AP Card

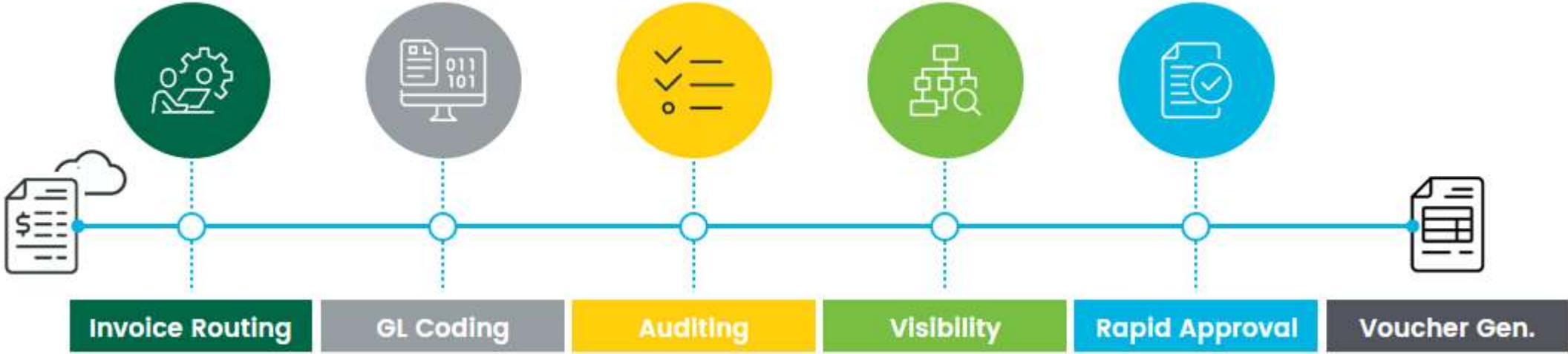
Payables Process



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.



Cloud-based AP Workflow



Payment Strategy



Reduce Costs



Efficiency



**Discounts &
Revenue Share**



**Risk
Mitigation**

Accounts Payable Analysis



Review current processes

- Invoice capture
- Payment approval process
- Payment types
- Payroll & expenses
- Fraud prevention
- Investments

Where do you want to go?

- How will you get there?
- Are you setting the bar high enough?

Let's map a strategy

- Process analysis
- Electronic & automation
- Financial & monetization
- Risk Management
- Measures & timelines

Apply the right tools

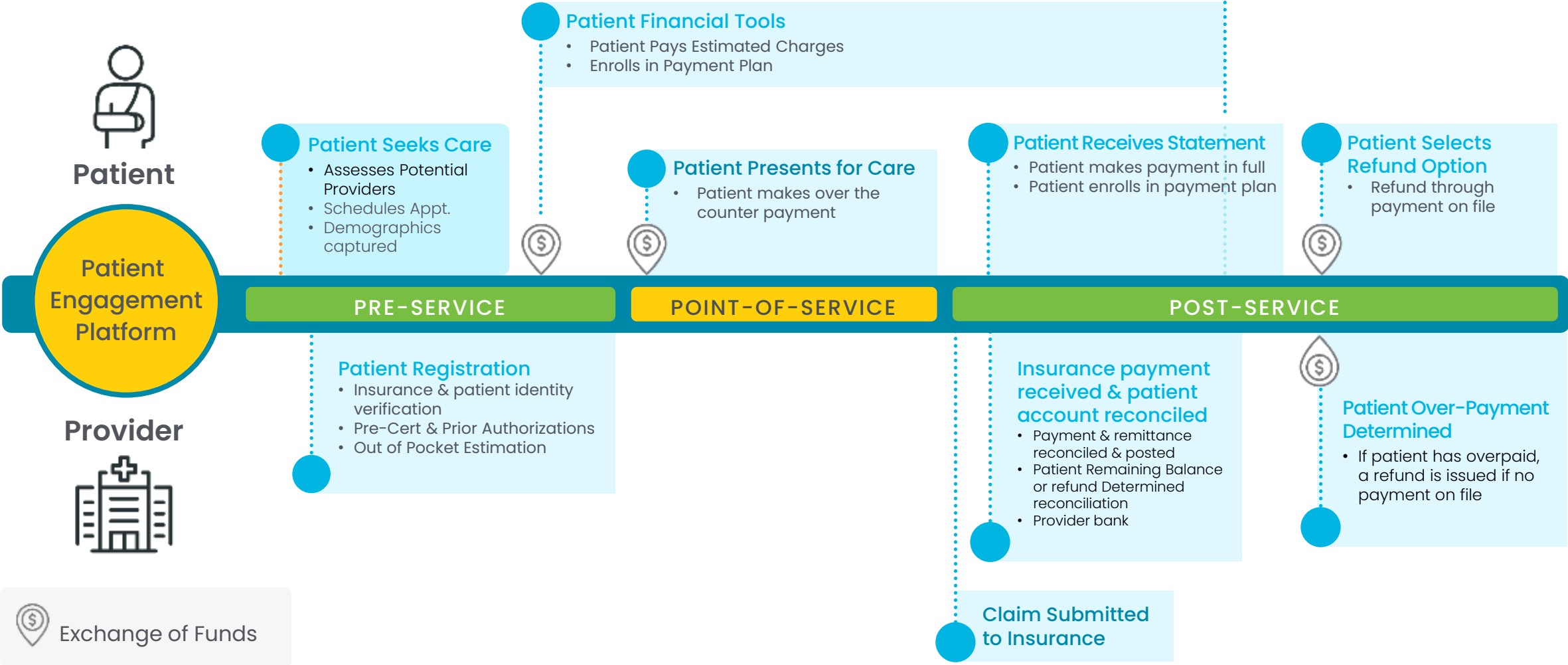
- Full product set
- Modular implementation
- Flexible product expansion
- Complete payment spectrum

Accounts Receivable 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?

The Patient Journey



Decoupled Data & Money

- Multiple payment types – card – physical & virtual, check, ACH, wire, instant payments
- Data needed to post the payment may or may not accompany the payment – different rails, payer portals, etc.



Patient Payment Platform



Consolidate online and POS providers to one solution



Resolve patient billing posting and statement issues



Automate check-in process



Payment posting file



Single solution to mitigate risks of data breach and reduce scope of required compliance



Process refunds through a single platform



Integrated estimation tool to collect for pre-service

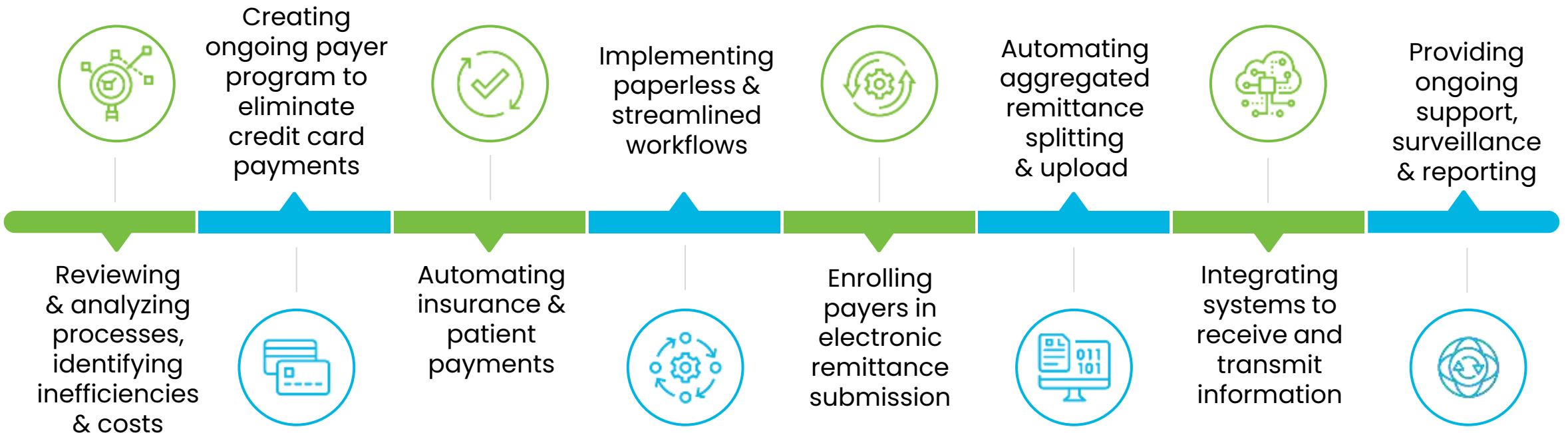


General ledger capabilities

Optimize Receivables



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



Healthcare Receivables Management



Recent Client Case Study

Total Savings

\$2.7M/year
Gross

\$1.9M/year
Net

Simplified Lockbox and account structure by **80%**

Average automated posting rate of 96% with limited use of EOB conversion

98% Auto matching rate for bank reconciliation

One-time accelerated cash flow of **\$25 million**

Reduction of payment processor fees **\$110k/mo.**

Reduced Lockbox volume by more than 50%

Performed bank changes & address changes during implementation

Implemented/trained **75+ staff members** during the pandemic with a remote workforce

Patient Refunds



Reduce costs of
issuing check



Streamline
process in Rev
Cycle & AP



Provide payment
options to
patient



Address
escheatment &
fraud concerns



Questions/Open Discussion

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) certifications. With 23 years of Treasury Management experience, Samantha offers her clients a wealth of experience in streamlining cash flow, improving efficiencies, and mitigating fraud.