20 YEARS

PHIMED TECHNOLOGIES

Welcome to AMPLIPHI

2026 CLIENT COLLABORATION AND MEETING

SPONSORED BY

Availity®

Commerce Bank® Member FDIC
Challenge Accepted.

Renkim
Print and Electronic Mail Solutions

Welcome to AmpliPHI

This year marks a meaningful milestone for PHIMED — 20 years of growth, innovation, and partnership alongside clients like you. Since 2006, we've been guided by a simple belief: **when our clients succeed, we succeed.** That belief is at the center of everything you'll experience here.

AmpliPHI was created with that same intention.

Over the next few days, our goal is to give you more insights and clarity. In an industry that continues to grow more complex, this time is designed to help you step back, challenge what's no longer working, and explore what's possible with the right systems, strategy, and support in place.

The sessions and tools you'll engage with are all rooted in helping you reduce friction, increase visibility, and operate with greater confidence. Most importantly, we hope you leave AmpliPHI with a renewed sense of control and transparency over your workflows, your data, and your long-term growth.

Thank you for being here and for being part of the PHIMED story.

Here's to the next 20 years!
The PHIMED Team

PHIMED TECHNOLOGIES

AMPLIPHI

2026 CLIENT COLLABORATION AND MEETING

Wednesday, April 15, 2026

2:00 - 5:00 pm	Registration	
5:00 - 7:00 pm	Welcome Reception	Nighthawk

Thursday, April 16, 2026

7:30 - 8:30 am	Breakfast	Tudor Ballroom
8:30 - 9:30 am	Opening Remarks	The Presidents Room
9:30 - 10:00 am	Lead With Curiosity: Creatively Building a Cybersecurity Culture	The Presidents Room
10:00 - 10:10 am	Morning Break	The Library Room
10:10 - 10:40 am	Availity | The Next Chapter of Revenue Cycle Management	The Presidents Room
10:40 - 11:15 am	CommerceHealthcare®: Innovations, Insights, and Best Practices	The Presidents Room
11:15 am - 12:00 pm	Luminus | The Silent Gatekeeper of Revenue: Why Provider Enrollment Is the Backbone of a High Performing Revenue Cycle	The Presidents Room
12:00 - 1:00 pm	Lunch	Tudor Ballroom
1:00 - 1:30 pm	No Surprises Act: Federal IDR Overview and Core Principles	The Presidents Room
1:35 - 3:25 pm	Breakout Sessions	

1:40 - 2:10 pm	**GROUP A** Reporting Essentials The Presidents Room	**GROUP B** Automations: Data Capture to Efficiency Tudor Balcony	**GROUP C** Maximize Guarantor Collections The Grille Room
2:15 - 2:45 pm	**GROUP C** Reporting Essentials The Presidents Room	**GROUP A** Automations: Data Capture to Efficiency Tudor Balcony	**GROUP B** Maximize Guarantor Collections The Grille Room
2:55 - 3:25 pm	**GROUP B** Reporting Essentials The Presidents Room	**GROUP C** Automations: Data Capture to Efficiency Tudor Balcony	**GROUP A** Maximize Guarantor Collections The Grille Room

3:25 - 3:35 pm	Afternoon Break	The Library Room
3:40 - 4:15 pm	Leveraging Technology to Increase Guarantor Collections	The Presidents Room
4:15 - 4:30 pm	Conclude	The Presidents Room
5:00 - 9:00 pm	20th Anniversary Celebration 5:00 - 6:00 pm Cocktail Hour 6:00 - 9:00 pm Dinner and Live Enerterntainment	The Starlight Ballroom

Friday, April 17, 2026

7:30 - 8:30 am	Breakfast	Tudor Ballroom
8:30 - 8:45 am	Welcome Remarks	The Presidents Room
8:50 - 9:40 am	Pre-Assigned Client Focus Groups	

	GROUP A The Presidents Room	**GROUP B** Tudor Balcony	**GROUP C** The Grille Room

9:45 - 10:30 am	Client Services Panel	The Presidents Room
10:30 - 10:45 am	Morning Break	The Library Room
10:45 - 11:15 am	Client Focus Groups Recap	The Presidents Room
11:15 - 11:30 am	Conclude	The Presidents Room

PHIMED TECHNOLOGIES

AMPLIPHI

2026 CLIENT COLLABORATION AND MEETING

Room Locations and Floor Information

Nighhawk

Lower Level

Access this location by the main guest elevators or stairs to the right of the elevator bank. Restrooms are located through a door at the back of the room.

- Wednesday, April 15 | Welcome Reception

The Grille Room

Floor 6

Access this location by the main guest elevators. Restrooms are located in the hallway before you enter the room.

- Thursday, April 16 | Breakout Sessions | Are You Maximizing Guarantor Collections?
- Friday, April 17 | Group C | Client Focus Group

The Library Room

Floor 3

Access this location by the main guest elevators. Restrooms are located in the foyer, before you enter the room.

- Thursday, April 16 | Morning and Afternoon Breaks
- Thursday, April 16 | Professional Headshots
- Friday, April 17 | Morning Break

The Presidents Room

Floor 3

Access this location by the main guest elevators. Restrooms are located in the foyer, before you enter the room.

- Thursday, April 16 | Main Sessions
- Thursday, April 16 | Breakout Sessions | Reporting Essentials
- Friday, April 17 | Main Sessions
- Friday, April 17 | Group A | Client Focus Group

The Starlight Ballroom

Floor 15

Access this location by a special elevator located to the left of the main guest elevators and the Town Co restaurant. Restrooms are located in the hallway, near the cocktail area.

- Thursday, April 16 | 20th Anniversary Celebration

Tudor Balcony

Floor 5

Access this location by the main guest elevators. Restrooms are located to the right when you get off the elevator.

- Thursday, April 16 | Breakout Sessions | Smarter Automation: From Data Capture to System Efficiency
- Friday, April 17 | Group B | Client Focus Group

Tudor Ballroom

Floor 4

Access this location by the main guest elevators. Restrooms are located to the right when you get off the elevator, in the hallway.

- Thursday, April 16 | Breakfast and Lunch
- Friday, April 17 | Breakfast

AVAILITY + PHIMED

Transforming Revenue Cycle Management

Accelerate reimbursement, boost cash flow, and deliver measurable financial results

Healthcare providers face mounting obstacles —rising denial rates, workforce shortages, and evolving security threats —all while striving to maintain consistent cash flow. Disconnected manual processes and fragmented revenue cycle management (RCM) solutions create workflow inefficiencies, payment delays, and payer abrasion, putting financial performance at risk.

Availity RCM empowers healthcare organizations to accelerate reimbursement, maximize cash flow, and achieve operational excellence. By uniting direct payer connectivity, intelligent automation, and proactive denial prevention, Availity delivers a resilient, future-ready RCM platform that drives measurable financial results.

Sitting at the intersection of payers and providers, Availity delivers what few revenue cycle vendors can, including:

- **Unmatched direct payer connectivity** reducing transaction delays and payer abrasion
- **Automation and AI-enabled workflows** that drive clean claim rates and operational efficiency
- **Flexible integration** with Epic and other electronic health records (EHRs) that allows RCM content to be integrated within existing workflows
- **A Rapid Recovery program** that ensures business continuity in the event of a cybersecurity event
- **Outstanding customer support** with 24/7/365 access to seasoned contact center associates based in the U.S.

Partnership Highlights

3K+

mutual providers supported

97%+

clean claim rate maintaining industry-leading performance

14

years of trusted collaboration

≤5%

denial rate - demonstrating exceptional results for our clients

1-3

days in claims processing time, dramatically accelerating reimbursement

Availity®
REVENUE CYCLE MANAGEMENT

Comprehensive Revenue Cycle Excellence

Availity RCM delivers seamless, integrated capabilities across every stage of the revenue cycle, empowering providers to optimize performance from patient intake to final reimbursement.

Pre-Service Optimization

- Advanced eligibility and Coverage Locator with near real-time and batch inquiries to identify active coverage early
- Automated eligibility workflows triggered by real-time or batch transactions to prevent downstream errors

Service + Encounter Management

- Automated claims creation and intelligent editing
- Seamless EHR integration for real-time, automated claim status and complete visibility

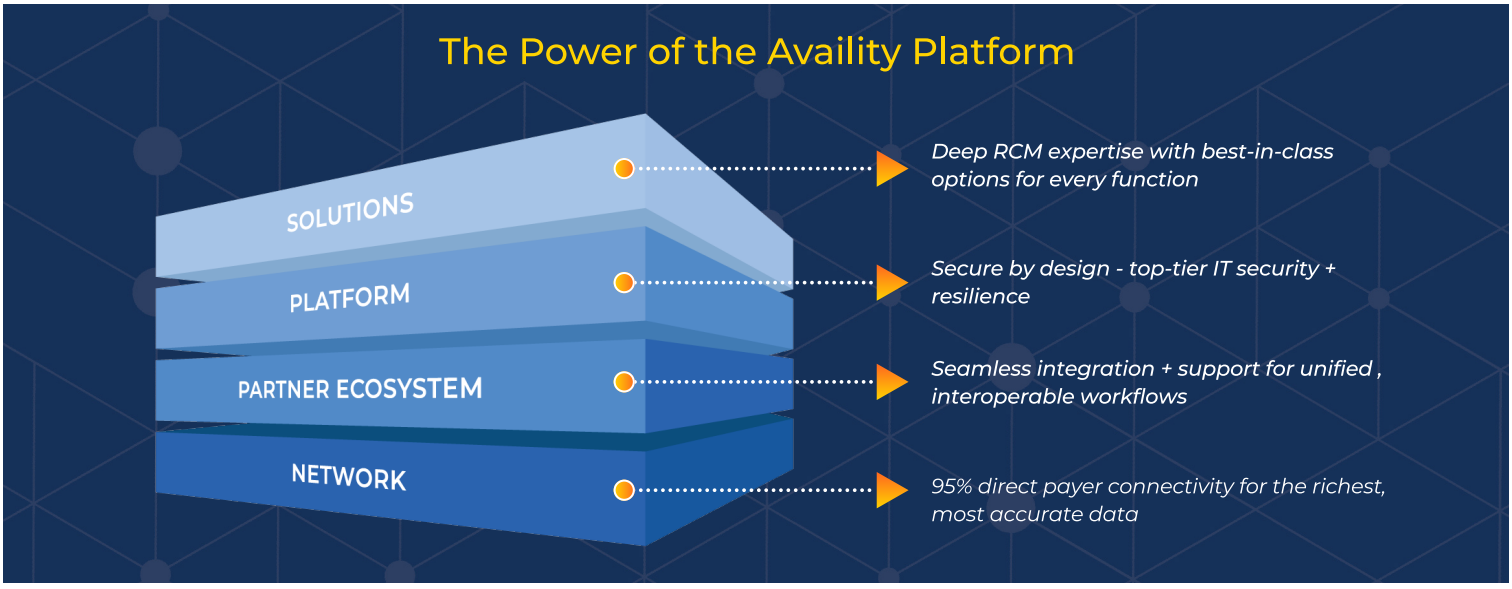
Post-Service + Adjudication Excellence

- Electronic remittance delivery with automated claim matching
- Proactive predictive editing and actionable analytics

Continuous Performance Improvement

- Dashboard insights for ongoing optimization
- Rapid recovery protocols to ensure business continuity and protect RCM operations

> We're seeing our A/R cycle operating a lot more efficiently. Availity has really helped us identify opportunities to improve our revenue cycle.
>
> *-Vice President of Patient Financial Services, Atrium Health*



Availity
REVENUE CYCLE MANAGEMENT

To learn more about Availity's Revenue Cycle Management offerings,
contact your account manager or visit us at Availity.com

Payments fraud:

Past lessons, present threats, future defenses.

Commerce Bank® Member FDIC | VISA

Payments fraud is defined as an intentional act to deprive someone or something of money or rights. As long as humanity has used currency-based payments systems, payments fraud has been a constant threat. According to Cambridge University Press, one of the earliest examples of payments fraud dates back to ancient Roman marketplaces. Fraudsters created fraudulent "fourrée" coins to imitate pure silver "denarii" coins. Fourrée coins had a base metal core with a thin silver coating meant to disguise it as a denarii coin. To prevent fourrée coins fraud, money changers developed the first "fraud mitigation" practices. They lightly filed the rim to expose the base metal core, weighing the coin against a known standard or noting a duller ring when struck.

Centuries later, as trade expanded across regions and new payment methods emerged, fraud evolved alongside them. Carrying coins was both cumbersome and exposed merchants to potential theft. According to the Association of Certified Fraud Examiners (ACFE), Arab merchants devised the "sakk," a financial tool akin to today's checks. It consisted of a paper instrument that facilitated the deposit of money in a bank in one country and its withdrawal in another. By the 16th century, this innovation had spread across Europe. However, criminals identified and exploited the system's flaw that handwritten checks were easy to forge and counterfeit. Fraud became so problematic that many regions prohibited this "modern" mode of payment. In 1762, British banker Lawrence Childs introduced the first printed checks, significantly reducing the risk of forgery and paving the way for modern check payments.

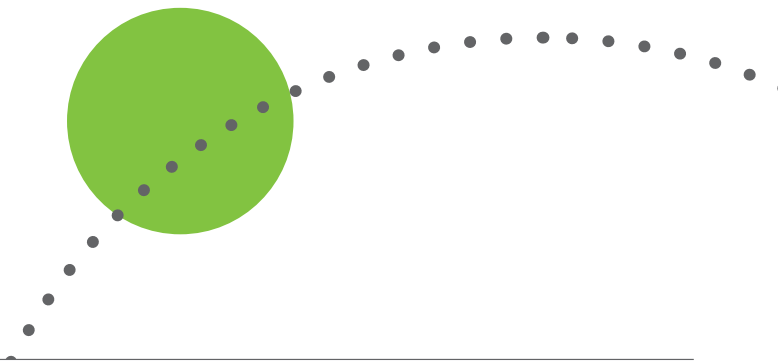
Since the start of the 21st century, the payments industry has shifted from paper-based systems to electronic execution and settlement. According to the Federal Reserve of Atlanta, ACH transfers grew from $20 trillion in 2000 to more than $90 trillion by 2021. The Federal Reserve of Kansas City attributes the growth to advances in technology and automation which provide convenience and reliability. However, this expansion has also created new opportunities for fraud. Fraudsters have developed new schemes such as creating fake vendors to infiltrate supply chain networks, using stolen information to access accounts, and impersonating coworkers to request payments.

Risks of modern banking are compounded by the removal of traditional human interaction from many payments processes. Detection relies on network-based monitoring and analytics. To adapt to new methods of fraud, maintaining the integrity of payments systems cannot simply be reduced to a checklist and must be integrated into business governance and operational frameworks with documentation, access controls, and audit trails. Advanced payments fraud mitigation tools now include tokenization-secured transaction architecture and AI-driven fraud detection models.

In commercial payments fraud, access to sensitive data is often the critical first step for fraudsters. By obtaining information such as bank account details, vendor records, invoice formats, employee email credentials, or internal approval workflows, criminals can convincingly impersonate legitimate parties and manipulate payments processes. This allows fraudsters to craft realistic invoices, spoof executive communications, or alter payments instructions without raising suspicion. The more accurate and detailed the stolen information, the easier it becomes for fraudsters to bypass security measures and execute high-value, unauthorized transactions.

Fraud Tactics and Mitigation Measures Over Time

Era/Period	Payments industry development	Common fraud tactics	Fraud mitigation measures
Pre-2000	Predominantly paper-based payments with gradual adoption of electronic transfers.	Check forgery, counterfeit currency, basic card theft.	Teller verification, signature matching, manual fraud checks.
Early 2000s	Growth of card-based payments, ATMs, and early online banking.	Card skimming, phishing, account takeover.	Chip-and-PIN rollout, encryption for online banking, multi-factor authentication.
Mid-2000s	Rapid shift toward real-time electronic settlement — a "silent revolution" in U.S. payments.	Large-scale breaches due to improper data storage.	PCI DSS implementation, enhanced monitoring, prepaid card anti-money laundering guidelines.
2010 – 2015	Expansion of mobile commerce, prepaid cards, and cross-border instant payments.	Synthetic identities, laundering using stored value cards.	Reload limits, customer verification requirements, large-scale adoption of real-time fraud analytics.
2016 – 2020	Global surge in e-wallet adoption and e-commerce.	Targeted malware, coordinated fraud rings.	Tokenization-secured payments architectures.
2021 – present	Development of Gen AI tools.	AI-driven fraud, deepfake-enabled identity theft.	AI fraud detection models to reduce false positives.



Fraud foundation.

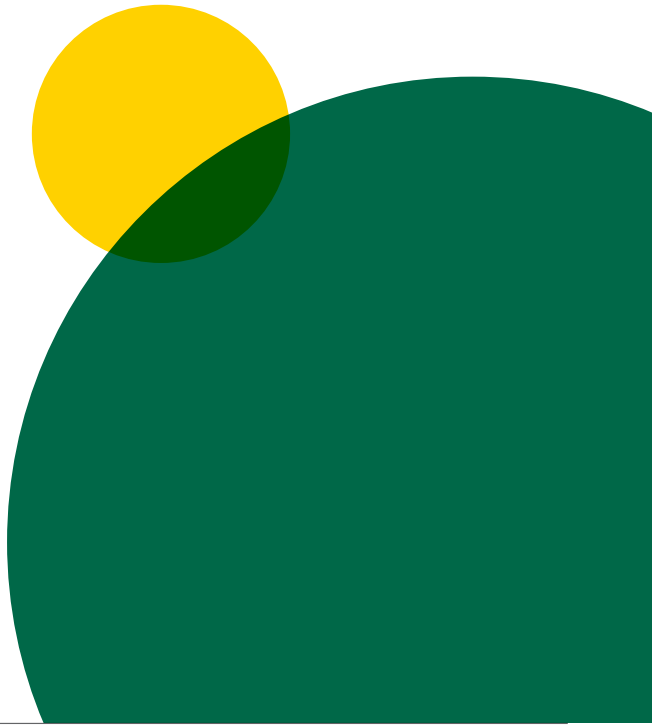
Payments fraud does not always use advanced technology, but rather sometimes uses low tech and exploits human behavior. By tricking employees into making mistakes or ignoring warning signs, fraudsters can bypass even the most sophisticated security systems. For businesses, these schemes can result in account breaches, unauthorized transfers, stolen customer data, and costly downtime. In many cases, successful fraud depends less on technical skills and more on exploiting everyday vulnerabilities.

1. **Physical information theft:** Dumpster diving is one of the simplest, yet most effective fraud tactics. By physically searching through trash for sensitive information, fraudsters can find passwords, pay slips, bills, and payments details they can use for identity theft or social engineering. Despite its low-tech nature, it works because many people and businesses fail to securely dispose of confidential documents.

2. **Social engineering:** Psychological manipulation targets people, not technology. Common social engineering tactics include business email compromise (BEC), phishing and vishing (voice phishing). These schemes often create a sense of urgency to override skepticism and exploit victims' weaknesses, desperation or inability to verify information.[1]

3. **Scareware:** This represents the technological version of social engineering, using fake security alerts to trick users into giving up sensitive information or installing malicious software. By blending technical deception with psychological pressure, fraudsters push victims into acting out of fear, often bypassing their usual caution.[2] As an example, "WinFixer/XP Antivirus" scareware campaigns used fake pop ups and bogus system scans to claim a victim's PC was infected. Users were urged to "fix" the issue by purchasing a fake antivirus and entering personal data. While consumers made up a majority of the victims, businesses that were affected took larger losses on average.

4. **Vendor/supply chain fraud:** This occurs when an intermediary, hired to identify and manage suppliers for international manufacturing, engages in deceptive practices that harm the buyer. Agents can misrepresent supplier capabilities, alter payments details, inflate costs or take kickbacks.



1. "Electronic commerce fraud: Towards an understanding of the phenomenon," Proceedings of the 38th Hawaii International Conference on System Sciences, 09/05/2025, link.
2. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures," *Applied Sciences*, vol. 12, no. 12, 09/05/2025, link.

Fraud monetization.

Information gained by exploiting human weaknesses fuels criminal activity against businesses. Fraudsters use stolen data to hijack existing accounts or coerce employees to execute ACH or wire transfers to fraudulent accounts.

1. **Account takeovers (ATO):** ATOs occur when fraudsters gain unauthorized access to a legitimate account, typically by using stolen credentials. Attackers validate credentials through targeted login attempts. Research shows some ATO attacks use bots for large-scale credential-stuffing, while other fraudsters have evolved into using "low and slow" credential cracking to avoid triggering detection and often attack on weekends when monitoring is reduced.[3]

   Once criminals gain access to accounts, they attain control of accounts by changing recovery information, registering new devices, or adding fraudsters as authorized users. Fraudsters monetize the account by transferring money to their accounts.

Real-life example: In November 2022, DraftKings suffered a credential stuffing attack, where criminals used passwords leaked from other sites to log in to users' sportsbook accounts. Once inside, they changed passwords, switched two-factor authentication to new phonenumbers and initiated withdrawals. DraftKings said 68,000 users' data had been exposed and roughly $300,000 was stolen. The company emphasized there was no evidence its systems were breached; the risk stemmed from password reuse across services.

3. "The Anatomy of Account Takeover," Imperva, 09/05/2025, link.

2. **Impersonation:** By posing as trusted executives, employees or vendors — sometimes using spoofed emails, hacked accounts or forged documents — fraudsters can trick businesses into approving unauthorized transactions. These schemes frequently create a false sense of urgency or authority to bypass normal verification processes, leading victims to send funds to fraudulent accounts or disclose sensitive payment information.

Real-life example: A 2020 Twitter vishing hack demonstrated advanced social engineering techniques when attackers contacted Twitter employees by phone, impersonating IT support staff. According to The Verge, fraudsters created a sense of urgency around a "critical security update" and convinced employees to provide access credentials. This breach affected high-profile accounts, including those of Barack Obama, Elon Musk and Bill Gates, resulting in a cryptocurrency scam that netted over $100,000.

3. **Vendor/supply chain fraud:** Sourcing agents inflate costs, take kickbacks from manufacturers, or even switch agreed-upon factories to cheaper, lower-quality alternatives without the buyer's consent. Such misconduct can result in defective goods, missed deadlines, and significant financial losses. The risk is particularly high in cross-border transactions where buyers rely heavily on the agent's local knowledge and have limited ability to directly verify the supplier's legitimacy.

Real-life example: A case detailed by Harris Sliwoski involved a U.S. company that engaged a sourcing agent in China to oversee the manufacturing of a highly specialized product. The agent presented a well-established and reputable factory, offering competitive pricing and strict quality control measures. The buyer, working from overseas, relied entirely on this agent's local knowledge. The agent secretly switched manufacturing to a cheaper and lower-quality facility and kept the cost difference as profit. When the goods arrived, they were riddled with defects, failed to meet technical specifications, and were ultimately unusable for their intended purpose. The buyer not only lost a substantial portion of their investment but also faced reputational damage and supply chain disruptions.

Fraud mitigation strategies.

Institutions and merchants must implement a multi-layered approach in mitigating fraudulent transactions. No single method can address every type of fraud, but combining complementary tools significantly strengthens security. Solutions such as multi-factor authentication, dual authorization, and account whitelisting all target different vulnerabilities in the payments process. Together, these measures help detect suspicious activity early, reduce the success rate of stolen card data, and card verification shifts the balance of security in favor of legitimate transactions.

Multi-factor and biometric authentication: 3D secure is an authentication protocol for online payments that adds a step in the process where the customer is verified by their bank before approval. Visa explains this process may happen silently in the background or may involve a brief prompt for the cardholder (face/touch ID, signing in to banking app, etc.). Since the bank checked and decided to approve or disapprove of the transaction, the liability for chargebacks falls onto them rather than the customer. This bank-side check allows for an additional layer of security and prompts to sign in or utilize face/touch ID helps introduce human verification measures into the authorization process.

Dual approval: Also known as dual authorization, describes a process in banking and financial transactions where two authorized individuals must review and approve a payment before it is executed. This control helps reduce fraud, errors and unauthorized transfers by helping ensure that no single person has full authority over the transaction. As explained by ProcessMaker, dual approval is widely used in corporate banking to safeguard against internal fraud, strengthen compliance, and maintain operational integrity, especially for high-value or sensitive transactions.

Vendor whitelisting: This is a security approach in which only validated and pre-approved vendors or payees, including specific verified bank accounts, are permitted to receive payments or access certain systems. This process builds on vendor validation and payee verification practices, helping ensure that every recipient has been vetted for legitimacy before being added to the whitelist. Allowing transactions only to trusted, verified recipients can significantly reduce the risk of funds being sent to fraudulent accounts. As explained by UMA Technology, whitelisting operates on the principle of default denial, meaning all accounts are blocked unless explicitly approved. This layered approach makes it a powerful defense against targeted attacks and social engineering scams in commercial B2B transactions.

Card verification: According to Visa, the two key fraud mitigation tools for online or phone card payments are Address Verification Service (AVS) and Cardholder Verification Value 2 (CVV2). AVS checks whether the street number and ZIP Code entered by the customer matches the information on file with the cardholder's bank. This helps merchants detect fraud when stolen card details are used without the correct billing address. CVV2 is the three- or four-digit security code printed on the back of cards, requested during remote transactions to confirm the buyer physically possesses the card. Together, AVS and CVV2 provide critical verification checks that help block unauthorized transactions and better protect businesses from payments fraud.

Emerging trends: Artificial intelligence (AI) and tokenization.

The payments fraud arms race is now entering the next phase. Two key trends are leading candidates to define the next phase: AI and tokenization. The creation of GenAI tools has simplified the process of creating deepfakes that can bypass human verification tests and pose significant risk to financial institutions and merchants. However, advances in AI technology will also prove to be crucial to the next generation of fraud mitigation, as synergy between AI driven models and dynamic tokenization will lead to constantly improving fraud recognition systems and data monitoring measures.

Bypassing human identification: The rise of deepfakes.

As GenAI tools have become more prevalent in recent years, fraudsters have found ways to use them in perpetrating increasingly sophisticated payments fraud. The U.S. Financial Crimes Enforcement Network (FinCEN) has warned about the rising use of deepfakes in identity fraud. Deepfakes allow fraudsters to fabricate realistic personas that can pass biometric authentications to gain access to financial systems and merchant platforms. According to the Forbes Technology Council, AI tools helped fuel a 700% increase in deepfake-related fraud attempts in the fintech industry in 2023.

As an example, in 2025, global design and engineering firm Arup became the victim of a sophisticated AI-enabled payment fraud scheme in Hong Kong. According to the World Economic Forum, scammers used deepfake technology to convincingly impersonate the company's Chief Financial Officer during a video conference. Believing the meeting was genuine, a staff member followed instructions to make multiple bank transfers, resulting in losses amounting to $25 million USD.

AI and tokenization: Developing the next fraud mitigation strategy.

Although AI has introduced a new threat in the world of payments fraud, it has also emerged as the analytical backbone of next-generation fraud mitigation systems.[4] Machine learning models and neural networks consistently outperform static, rules-based systems. These models can process millions of transactions almost instantaneously by identifying anomalies invisible to manual approaches. Importantly, these models are adaptive and continuously refine their parameters to match evolving fraud patterns, making them more resilient to emerging attack tactics.

Industry leaders are applying AI not only for detection, but also for frictionless customer experience (CX). According to PYMNTS, AI tools such as Featurespace utilize real-time behavioral biometrics and adaptive scoring to intercept suspicious transactions before authorization, without disrupting legitimate purchases. These tools also allow for contextual decision-making, risk-based authentication, and personalized fraud alerts, reducing false positives and enhancing customer trust.

Dynamic tokenization replaces sensitive account information with a token, or a random string of characters, for a specific transaction. Transaction-specific tokens expire immediately after use. This not only reduces the attack surface, it also integrates smoothly with AI-powered fraud analytics, allowing models to process tokenized data enriched with behavioral metadata without compromising privacy.[5] By safeguarding payment information, tokenization helps businesses build customer trust, streamline operations, and reduce the cost of managing data breaches.

The synergy between AI and tokenization is a crucial aspect of the next generation of fraud mitigation. Tokenized transaction streams can be shared safely across institutions for collaborative AI model training, enabling industry-wide fraud pattern recognition without breaching data protection laws. Conversely, AI can monitor token usage patterns to detect anomalies and automatically revoke tokens that appear compromised. This dual-layer strategy strengthens defenses, ensuring that even if fraudsters bypass detection systems, the stolen data remains unusable.

4. "Smart Credit Card Fraud Detection Using Machine Learning," Rochester Institute of Technology, 09/05/2025, link.
5. "The Use of AI in Combating Payment Gateway Fraud: A Comprehensive Analysis,"ResearchGate, 09/05/2025, link.

What might the future hold?

From the earliest currency-based exchanges to today's electronic payments systems, fraud has been a constant companion to innovation. Many of the most effective fraud schemes today are relatively low-tech, leaning on social engineering and other human vulnerabilities to gain access to systems and information. As technology evolves, AI tools can develop deepfakes that can bypass human verification measures. As fraudsters evolve the ways they access sensitive data, mitigation tactics will continue to evolve in step. Effective use of AI-driven fraud recognition models along with the use of dynamic tokenization are creating dual-layer protection that can effectively respond to emerging threats. Ultimately, the ongoing battle between payments fraud and fraud mitigation shows no signs of slowing.

CommerceHealthcare®

4 Healthcare Financial Trends

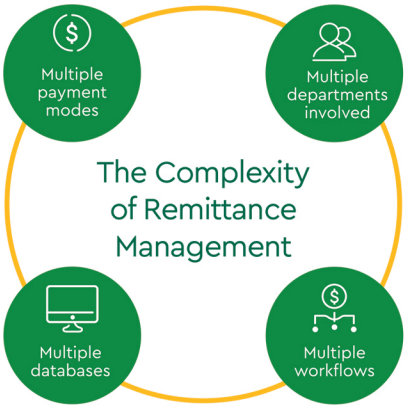
for 2026

ACCELERATING AUTOMATION IN FINANCE

Fully removing manual processing of high-volume administrative transactions could save healthcare

$18 billion.[1]

Significant opportunities exist to address continuing complexity in processes such as remittance management that create costly delays, errors and omissions.



EMERGENCE OF REAL-TIME PAYMENTS TRANSACTIONS

Healthcare logged

141 million ACH payments

in Q3 of 2025, up 6.8%.

↑ 6.8%

The Clearing House's Real-Time Payments network processed

115 million transactions

across industries for

$405 billion in Q3 of 2025.[2]

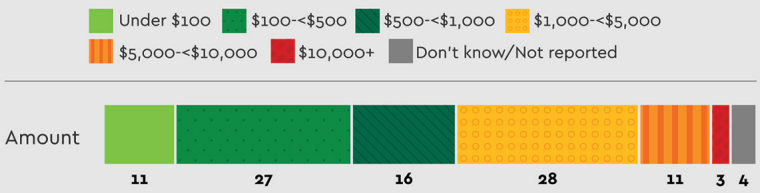
Real-time processing is transforming healthcare transactions, including:

- Immediate identification of coding and billing issues
- Real-time credit decisions
- Intelligent payment routing
- Smart contracts using blockchain technology

AFFORDABILITY A HEADLINE ISSUE IN 2026

Almost **6 in 10** healthcare borrowers took on debt of **$500 or more** within the past year.[3]

How Much Money Did You Borrow?



source: Gallup/West Health

Patient financing totaled **$16 billion** in 2024 as steady demand fueled five-year compound annual growth of 3.2%.[4]

↑ 3.2%

Expanded payment plans should offer:

- Longer durations and larger dollar amounts covered.
- Zero interest rate lines of credit.
- Financing based on pre-service cost estimates.

EMPHASIS ON COMMUNICATION, TRANSPARENCY, TECHNOLOGY TO IMPROVE PATIENT FINANCIAL EXPERIENCE

8 in 10 adults are unaware of their care costs in advance.[5]

of patients received estimates over the past year. Accuracy slipped from **78% to 71%.**[6]

are more likely to pay their bill on time when providers text from a recognizable 10-digit phone number.[7]

Voice-initiated mobile payments are **growing nearly 16% annually** through 2029.[8]

1. CAQH, *2024 CAQH Index*, February 21, 2025.
2. Boston Consulting Group, *Global Payments Report 2025: The Future Is (Anything but) Stable*, September 2025.
3. Gallup, "Americans Borrow Estimated $74 Billion for Medical Bills in 2024," March 5, 2025.
4. IBIS World, *Medical Patient Financing* in the US, December 2024.
5. Gallup, "Few Americans Know How Much Their Healthcare Costs," January 31, 2024.
6. Experian, *2025 State of Patient Access Survey*, April 2025.
7. Artera, "Trends in Patient Engagement," August 29, 2025.
8. Research and Markets, *Voice-Based Payments Market Report 2025*, September 2025.

CommerceHealthcare®

CommerceHealthcare® solutions are proivded by Commerce Bank.

Read the full Trends Report at:

HEALTHCARE FINANCE TRENDS FOR 2026: A DYNAMIC MIX OF OPPORTUNITY AND RISK

PHIMED TECHNOLOGIES

AMPLIPHI

2026 CLIENT COLLABORATION AND MEETING

Thank You for Joining Us

We're grateful you took the time to be part of these conversations and this experience. As we look ahead, your perspective matters and is an important part of how we continue to evolve.

Please take a moment to scan the QR code and complete our post-conference survey.

20 YEARS

PHIMED TECHNOLOGIES

PHIMED.COM