Redefining Secure Payments

SOLUTIONS FOR A SEAMLESS, SECURE HOMEOWNER EXPERIENCE

CINC

Introduction

Hurricanes, floods, wildfires—community association management companies are no strangers to unpredictable and costly threats. Boards plan ahead, perform regular inspections, and invest in preventative maintenance because ignoring risk doesn't make it go away.

Today, HOAs and Community Association Management (CAM) companies face another ever-present threat that can be just as disruptive: cyberattacks. Increasingly sophisticated and amplified by artificial intelligence, cybercrime has become a persistent force that quietly targets the systems CAMs rely on every day—especially payments.

CAM companies are an attractive target for bad actors. Many operate lean teams, manage large volumes of financial transactions, and rely on legacy processes. Without a cybersecurity strategy or modern payment controls, even well-run organizations can be left exposed.

As high-profile breaches dominate headlines, residents are increasingly concerned about how their personal and financial data is handled. Trust, once lost, is difficult to rebuild.

In community management, warning signs like aging roofs, outdated fire systems, or deferred maintenance are taken seriously—requiring action before catastrophe occurs. It's time to treat payment security with the same urgency and discipline.

> "I recently worked with a CAM company whose email system was compromised. Before migrating to CINC Systems, they had been using email to collect and transfer ACH information. **What started as a simple breach quickly escalated into a full review of their cybersecurity controls and insurance coverage**."
>
> Gabriel Valentino, Director of Payment Adoption, CINC Systems

Payment Fraud's Impact on CAM Companies

Lost Funds

Admin Burden

Loss of Trust

Legal Impacts

Where Payment Fraud Takes Hold

Paper Checks

For CAM companies, every check in circulation represents both financial risk and administrative burden.

Paper checks remain a primary target for payment fraud, as criminals can alter payees, amounts, or routing information with minimal effort. Checks are vulnerable before they're ever processed, since mail theft from residential mailboxes and payment dropboxes has become increasingly common. When fraud occurs, homeowners often don't realize it until days or weeks later when reviewing bank statements, delaying response and recovery.

Checks also create operational drag. Investigations require manual reconciliation, paper trails, and coordination across banks, homeowners, and vendors. Compounding the risk, recent postal processing changes have introduced new delays between when a check is mailed and when it is officially processed—increasing risk of exposure and late payments.

> "Anyone with graphics software and a high-quality printer **can readily turn out counterfeit** checks."
>
> David Lott, payments risk expert in the Atlanta Fed's Retail Payments Risk Forum

ACH Payments

While faster and more efficient than checks, ACH payments introduce their own risks—especially when controls are weak.

A significant share of payment fraud targets ACH debits and credits, often exploiting gaps in authorization, access controls, or internal processes. In CAM-managed ACH programs, the management company bears responsibility for safeguarding bank account data and responding to fraud, errors, or compliance issues.

Risk often stems from how sensitive data is handled. ACH authorization forms containing homeowners' bank account information are commonly stored in file cabinets, shared drives, or unencrypted systems accessible to multiple employees. These practices increase the likelihood of internal misuse, external breaches, and compliance failures.

The Rising Tide of Cybercrime

In 2024, losses from cyberattacks reached an estimated $9.5 trillion, making cybercrime the third-largest economy in the world.

Widely available AI tools have lowered the barrier to entry, allowing attackers to automate reconnaissance, generate highly personalized phishing messages, and exploit public data with minimal effort.

Attackers can now run thousands of simultaneous attempts, learning and adapting with each pass. AI-powered password-cracking tools can compromise the vast majority of common passwords in weeks.

As organizations rely on more software platforms, integrations, and vendors, the attack surface expands. Bad actors increasingly exploit third-party tools and vendors as entry points, knowing that interconnected systems can provide access far beyond a single weak link.

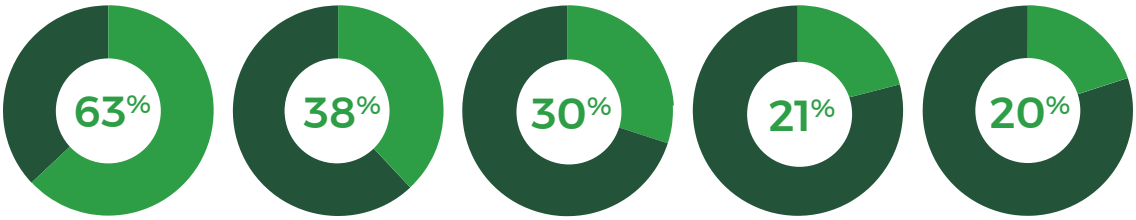
81% of common passwords can be cracked using AI tools **within a month**.

70% of attacks enter through **vendors or third-party systems.**

Where Most Organizations Stand

According to Accenture's 2025 State of Cybersecurity report, 63% of organizations fall into the "Exposed Zone." This means they lack both a clear cybersecurity strategy and the practical safeguards needed to consistently protect their systems—making them far more vulnerable to modern cyber threats.

Prevalence of Payment Fraud Attempts



Source: The Association for Financial Professionals 2025 Payments Fraud and Control Survey

The Urgent Need for Secure Payment Solutions

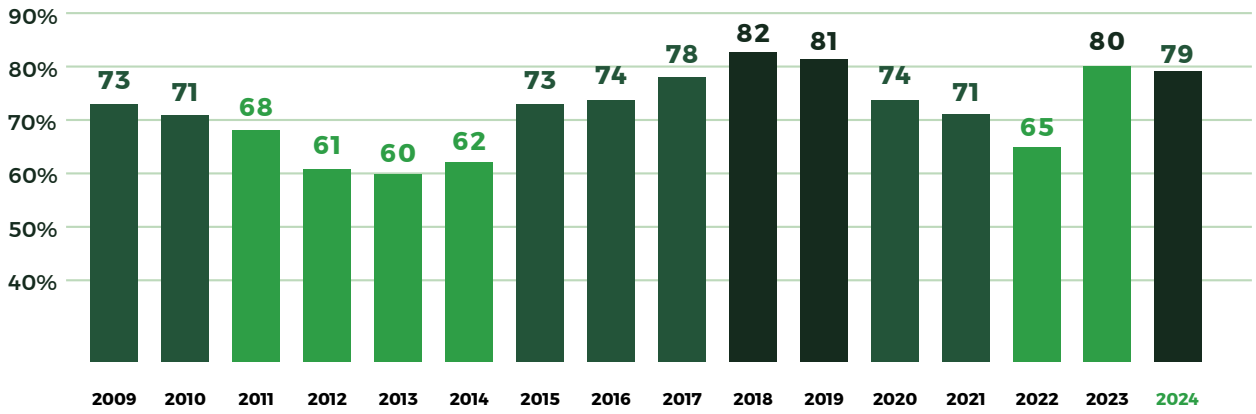
Nearly 8 in 10 organizations reported having been targets of payment fraud activity in 2024. Profit-driven cybercriminals and nation-state adversaries can cripple school systems, police departments, healthcare facilities, and private sector organizations. HOAs are even more vulnerable, because they're known for being low-tech.

Yet, many HOAs continue to use outdated systems and processes, putting homeowners and their sensitive data at risk. HOAs and CAM companies that don't comply with local and state data privacy laws could also face serious legal ramifications.

CAM companies need to take these risks seriously and take action, starting with payment systems. Here's what you'll need to consider to safeguard sensitive homeowner data and your bottom line.

> "Property management firms that store **payment data in unencrypted systems face significant security and compliance risks,** leaving them highly vulnerable to data breaches and fraud."
>
> Tom Kiernan, CINC Systems Board Member, Co-Founder and Former CEO of ClickPay

Percent of organizations that experienced attempted and/or actual payment fraud



Source: 2025 AFP Payments Fraud and Control Survey Report

Safeguarding Payments & Your Bottom Line

HIGHER RISK PRACTICE	MORE SECURE BEST PRACTICES
ACH debit programs that require **collecting and storing homeowner bank account numbers**	Switch to **homeowner-initiated recurring eChecks**, shifting sensitive data handling to secure third-party providers.
Reliance on paper checks for homeowner payments	**Sunset paper checks in favor of electronic payment methods** to reduce theft, loss, and fraud exposure.
Paying vendors by paper check	Use electronic **vendor payments or secure payment providers** that assume check-related risk.
Broad or unrestricted employee access to stored bank account information	**Enforce strict, role-based access controls** so only authorized personnel can view sensitive data
Single-factor login credentials for staff systems	Enable **multi-factor authentication** (MFA) across software and payment platforms.
Homeowners relying on **basic login credentials** for payments	Encourage **homeowners to enable MFA** within their banking and payment tools
Static or **weak employee passwords**	**Require employees to use secure passwords** and change them regularly. Platforms like CINC Systems can automatically prompt users.

eCheck: A Safer Way to ACH

ACH debit and eCheck are often used interchangeably, but the key difference is that eChecks are initiated by the homeowner, while ACH payments are authorized by the homeowner but initiated by the management company.

Homeowner initiates payment. eCheck information is not handled or stored by the management company, but by a secure third-party provider.

Encryption adds another security layer. Even if a hacker obtained access to the database, sensitive homeowner data remains inaccessible without the private keys necessary for decryption.

Enterprise-grade CAM security you can trust.

At CINC Systems, trust is the foundation of everything we do. CINC follows a proactive, defense-in-depth strategy to safeguard your data. Our systems are monitored 24/7, regularly tested, and updated to address emerging threats.

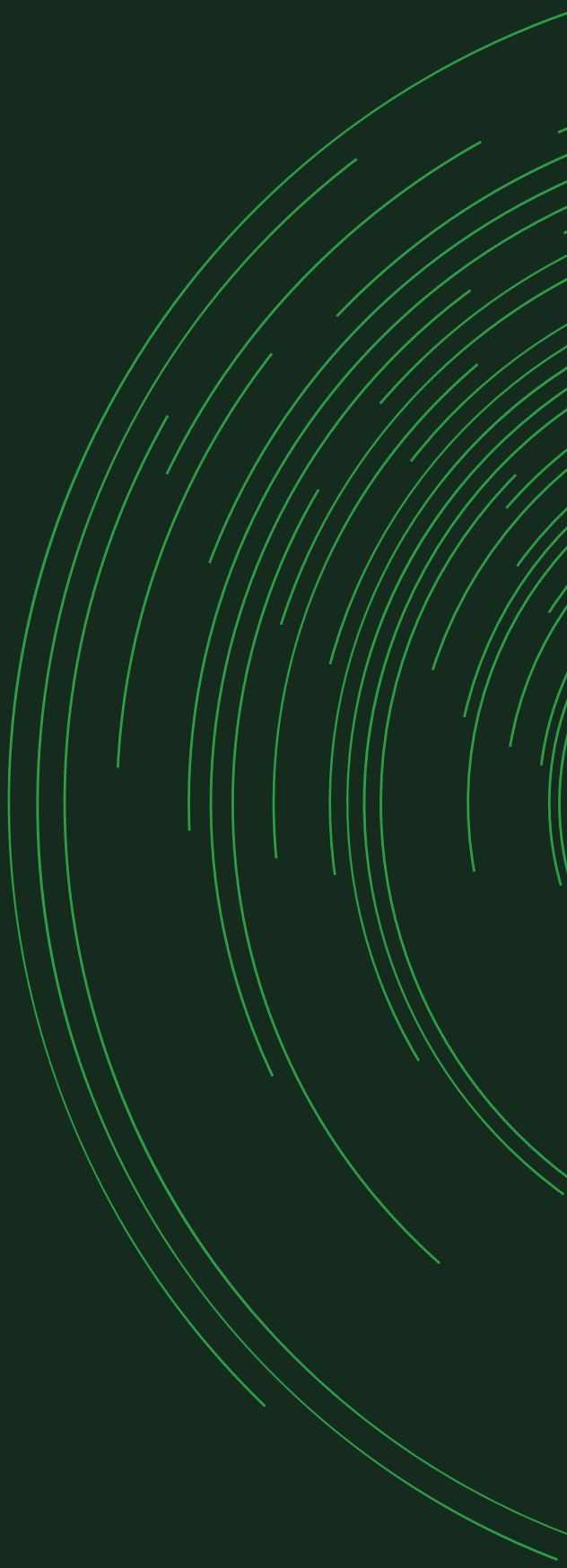
- **Secure by design:** Bank-level encryption protects data in transit and at rest.
- **Controlled access:** Role-based permissions and multi-factor authentication limit exposure.
- **Modern digital payments:** Reduce reliance on checks and manual, high-risk processes.
- **Built for compliance:** SOC 2 Type II certified, hosted in secure U.S. data centers, and regularly audited.
- **Operational resilience:** Automated backups and secure cloud access keep systems reliable and available.

> “The best way a property management firm can protect homeowner’s data from cyber criminals is by **implementing a secure, end-to-end digital payment solution.”**
>
> Alan Cohen, General Manager of Financial Services at CINC Systems

From Payment Risk to Peace of Mind

Whether you’re an existing CINC customer looking to increase digital payment adoption or a CAM company exploring best practices, our payment experts are here to help. CINC will walk you through proven approaches to reducing payment risk, and how CINC’s secure payment solutions deliver peace of mind for both your team and your homeowners.

CINCSYSTEMS.COM/CONTACT-US



CINC

CINC Systems is the only end-to-end, AI-powered community management platform built to make the value of professional management visible. CINC reduces back-office burden for community association managers while giving residents and boards a modern self-serve experience. Trusted by 1,000+ community association management companies representing 50,000+ associations and 6M+ residents nationwide,

CINC unifies accounting, banking, portfolio operations, and resident engagement in one connected platform.