Securing Financial Institutions

FOUR WAYS MODERNIZING PHYSICAL ACCESS CONTROL PROMOTES STRONG NETWORK SECURITY

The financial services (FinServ) sector must meet a high bar when it comes to security. Facing constant risk of physical and cyber breaches, financial institutions must safeguard not only their employees and guests at physical locations, but also vast monetary resources, along with the data stores of customers' financial and personally identifiable information (PII).

Adding to the risk, legacy and fragmented physical access control systems (PACS) persist as financial institutions largely manage multiple facilities across regional, national, or global locations. At the same time, the rise in cybersecurity threats has elevated the stakes as physical and logical access increasingly converge, requiring Security and IT team collaboration. Without collaboration it becomes easier for attackers to compromise physical access to networks and digital resources, leading to loss of institutional assets, compromised PII, and damage to an organization's brand reputation.

> *"The financial industry is highly regulated and we're required to protect our customers' information. When we don't it can be very expensive and very embarrassing, with high reputational risk."*
>
> ***—A FinServ Security Professional, Los Angeles, CA***

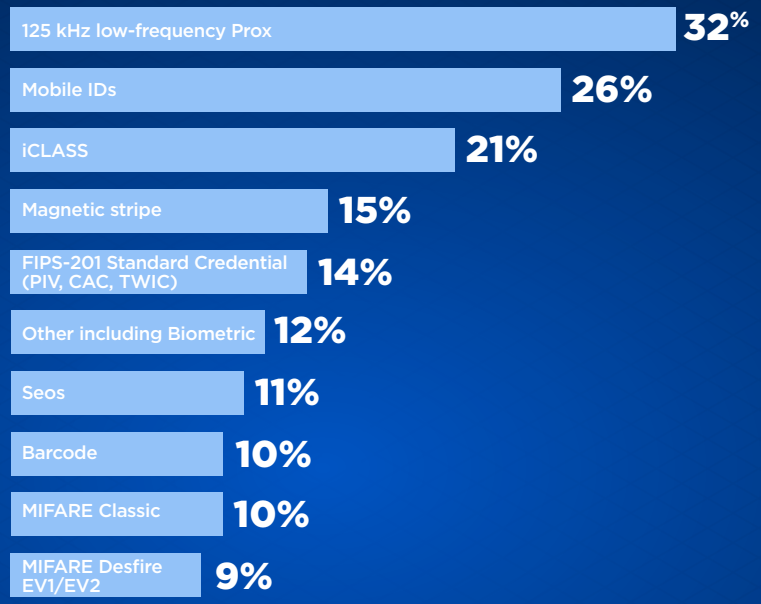
To mitigate the growing cyber and physical security risks, FinServ institutions must migrate from legacy access control technology to more secure solutions, like high-frequency smart cards and mobile-enabled, multi-tech readers. Such a move supports the convergence of physical and logical access control—securing physical spaces containing critical data while boosting network security, a key requirement in the industry.

A Snapshot of Access Control Technology in FinServ Today

The current credential technologies landscape features a mix of legacy solutions with some modern elements. In some cases, institutions may utilize heterogeneous solutions to address the varied levels of security needed to protect both high- and low-risk areas. Outer perimeters like parking garages and elevator access, often managed by a third party, may employ 125 kHz low-frequency prox or magnetic stripe, while the office suite requires a more secure iCLASS® or Seos® credential, managed by the institution. Layers of access control may be implemented on a single card depending on the party controlling access to the space, or the sensitivity and restrictions required for that line of business.

But security professionals know that employing legacy credentials like prox and magnetic stripe fall short of their desired threat mitigation. According to a survey of 96 FinServ security and IT professionals conducted by ASIS International and HID Global, just 45 percent say their current solutions—including credentials as well as readers and controllers—satisfy essential requirements, and a slim 14 percent say their current deployments exceed requirements. More than 50 percent say their readers and controllers are three to six years old or older. More worrisome is the following: under six percent say their existing physical access control system meets or exceeds their current and planned requirements.

Which PACS credential technologies does your organization currently support? (select all that apply)



> *We're using a multi-tech, multi-payload Seos Elite card, which incorporates two other technologies. This allows us to be able to communicate to different types of readers depending on our environment or location.*

—A FinServ Security Professional, Los Angeles, CA

PACS Challenges in FinServ

Security professionals recognize the inherent threat embedded in their legacy solutions. “We knew a number of years ago that prox was insecure,” said one team leader of physical security technical support at a Chicago-area financial services institution. “We saw a live demo of a card cloner. It took the guy under a minute to clone a prox card that we owned and distributed, and have the credential added to another prox card that granted access and looked identical to the original.”

While FinServ is under intense pressure to secure PII and other sensitive and confidential data, especially given the high degree of media attention around cyber breaches, brand reputation and trust is also critical to maintaining and growing their customer base. “It’s not just about the money, but it’s also about brand reputation, brand trust,” said Rob Murphy, CPP, CLSD Security, Risk, and Crisis Strategist.

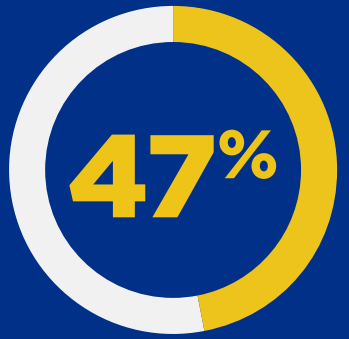
Yet, according to the survey, 32 percent of respondents were still utilizing 125 kHz low-frequency prox and 15 percent magnetic stripe credentials for at least a segment of their user base.

Many financial services organizations suffer from a disaggregated approach to PACS.

> *Many companies are using disparate systems, typically due to acquisitions or mergers where a subsequent upgrade to a single, uniform platform or solution has not taken place.*

—Rick Winter, HID Global End User Business Development Manager-Finance, PACS

Disparate controls operate independently in different locations, challenging coordination and communication. Especially when IT and Physical Security departments share a budget, such systems generate a burdensome administrative load for both security and IT teams and can drive high-level managerial challenges. Some 47 percent of FinServ security professionals cite project prioritization and alignment as a major hurdle where budget is shared, while almost 44 percent have concerns about managing multiple credentials in multiple systems, according to the survey. The inability to manage PACS seamlessly across the organization can also result in security vulnerabilities.



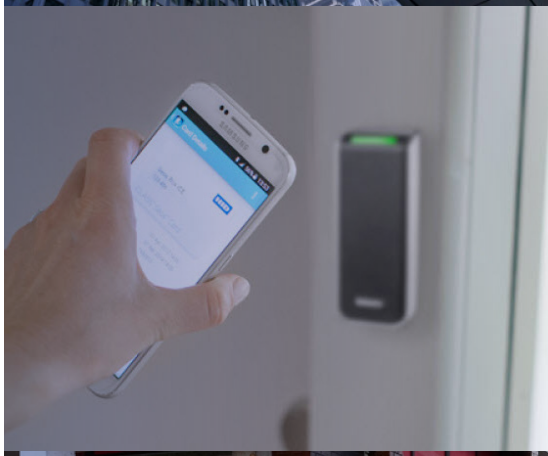
Say Security and IT prioritization and alignment are major hurdles when budget is shared

Say managing multiple credentials in multiple systems is a concern

Varied Needs on Premises and Across Locations

When current solutions come up short, it's partly a result of PACS complexity in the FinServ arena. Security professionals increasingly are tasked to secure disparate facilities in diverse geographies with a range of credentials at each location.

With this complexity comes the need to work with third-party applications, as well as with outside entities such as landlords, building managers, and vendors in order to effectively support PACS from the parking garage to the office suite to the server room. These layers require PACS configurations that restrict or allow an individual to access different properties, or different spaces within a single facility, based on business role.



Where Dual-Factor Falls Short

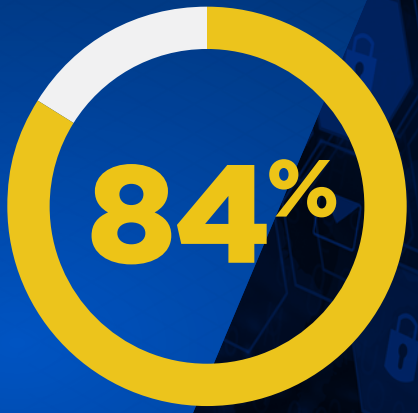
Some have turned to dual-factor authentication as a way to bolster the efficacy of existing systems.

While dual-factor authentication will enhance security in some use cases, there are certain applications in which this approach fails to meet basic needs. Suppose for instance, a PACS system requires a combination of a card and PIN. A PIN can be stolen just by looking over someone's shoulder, and a low-frequency card may be easily cloneable. "Anyone with $30 can go out and buy a badge cloner for a traditional prox card," Murphy said.

Winter agreed that a dual-factor authentication or low-frequency technology in concert with keypads is not sustainable. "This may be a short-term fix, but it's not a long-term solution to prevent future vulnerabilities," he said.

Taken together, these intrinsic vulnerabilities combine to make some dual-factor scenarios a less-than-complete fix for the current state of PACS risk. Equally worrisome, a false sense of security at the PACS level can lead to lapses in security at the network level, thus heightening the cyber risk, especially when 84 percent of those surveyed are still using username and password for access to network applications.

A false sense of security at the PACS level can lead to lapses in security at the network level, thus heightening the cyber risk, especially when 84% of those surveyed are still using username and password for access to network applications.



of those surveyed use username and password for network applications

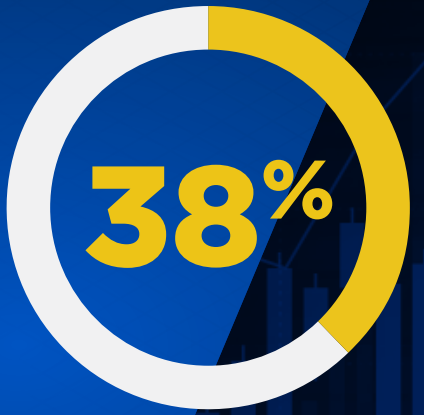
Budgetary Constraints

While many FinServ security professionals understand the need to upgrade, some may be biting off too much at once. By envisioning large systemic overhauls, they've raised budgetary red flags and let the perfect get in the way of the good. In fact, 38 percent of survey respondents say cost is the biggest obstacle to PACS upgrades.

Many face challenges in securing and managing budgets in support of PACS. The survey found that for projects that integrate physical and logical access, 24 percent of organizations tap the physical security budget, while 22 percent draw from IT funding. Another 20 percent say physical security and IT share a technology budget, while 22 percent say it depends on the project.

> *"Global Financial Institutions are now experiencing enhanced operational efficiencies; driving down operational costs, improving user convenience and protecting their businesses from potential vulnerabilities and reputational damage. Deploying and migrating a phased update to secure mobile access solutions is removing legacy vulnerabilities and seamlessly integrating into their access control systems."*

—Peter Walsh, Global Business Director- Finance Vertical Leader HID Global



Say cost is the biggest obstacle to upgrading PACS systems

Upgrading to Secure Technology, Including Mobile, Is a Must

Too often, PACS upgrades are put off on the grounds that the perceived threat doesn't warrant the expenditure. According to the survey, 45 percent of respondents say their institution has no current upgrade plan. If high-risk events occur only infrequently, upper management may not have a sense of urgency, so it's up to security leaders to make that argument.

> *"A lot of the work is putting a case together for the long-term health of the company, answering questions about the risks the project addresses and the beneficial impact."*
>
> ***—Rob Murphy, CPP, CLSD Security, Risk, and Crisis Strategist***

At the same time, security and IT professionals on the front lines must maintain constant vigilance over their physical and logical access control systems. According to the survey, their concerns related to access control include cyber breaches, insider threats, and physical security breaches. They worry too about new pandemic-driven security needs and the rising call for touchless access.

Top 5 Perceived Threats

1	Cybersecurity breaches	24%
2	Insider threats	22%
3	Physical security breaches	21%
4	Pandemic/ emergency/natural disaster	18%
5	Too many policies	7%

As security professionals seek to make the case for enhanced security, mobile credentials play a key piece in the modernization journey, and many FinServ organizations have already taken the first steps. Some 26 percent will upgrade to mobile-enabled readers within the next one to three years, and eight percent have already done so. Another eight percent will deploy mobile-enabled readers in less than a year, while the remainder will upgrade in greater than three years or don't have plans at this time.

> *"We installed mobile modules on every reader in our system. We had it vetted by the same IT team who exposed deficiencies with the prox system. They gave it a passing grade and we are really happy with the results."*

—A FinServ Security Professional, Chicago, IL

Upgrade Plans to Mobile Access

Will deploy within the next 1-3 years	**26%**
Already upgraded	**8%**
Will deploy in less than 1 year	**8%**
Will deploy in the next 3+ years	**8%**
Currently in the process of upgrading	**4%**
No current upgrade plan	**45%**

Why Mobile?

While institutions transition to mobile-enabled, multi-tech readers as an initial step, mobile credentials offer the possibility of instantaneous, over-the-air provisioning, a key need during the era of social distancing and beyond.

Administrators can deploy and revoke mobile credentials at the push of a button, without the need for a face-to-face encounter, which also facilitates touchless interactions. Photo identification on mobile phones can also take the place of printed photo IDs, where employee images are often out of date or easily spoofed.

Moreover, mobile credentials help minimize the cyber risk inherent in legacy systems. While users by nature tend to be tethered to their mobile phones, they also employ the passcode, fingerprint or facial recognition features inherent to the phone, creating increased security whether used to access a building or a network. It's also far more difficult to clone a mobile credential, for example, than to spoof a card. By making it harder for malicious actors to access key spaces and systems, mobile-based authentication can reduce the overall cyber risk, while also helping to minimize insider threats.

MAKING THE MOST OF MOBILE

- *Mobile credentials offer over-the-air provisioning*
- *Mobile credentials are difficult to clone*
- *Better physical security supports better logical security*

Greater PACS Alignment Drives Tighter Security

FinServ could begin to remediate the PACS challenges by eliminating the fragmentation among its security systems. Greater alignment of solutions across the enterprise would lead to better manageability and tighter security all around.

Some already see the potential advantage in pursuing a more uniform solution set. “As we replace all of the readers in a particular facility, now we can flip that facility from prox to Seos credentials, and once we get it completely on Seos, then we can turn off the prox portion,” Murphy said. “Now that entire facility is much more secure.”

Access Control Is Merging With Identity Management

Along with a more unified PACS deployment, security and IT leaders can begin to pursue the merging of access control and identity management.

In the evolving PACS technology landscape, access control represents just a part of the equation. The same credentials that open doors and grant entrance to the parking garage can be leveraged to manage a user's identity to provide logical access—to release sensitive documents from a public printer, for instance, or to log into the network.

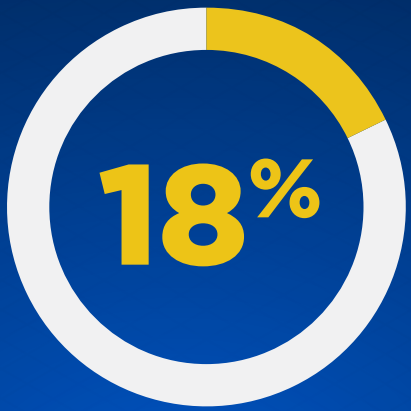
There are inherent advantages in the melding of physical access and identity management, one security expert said, "I want to have that 360-degree view of an individual, I want to understand their physical and logical access as well as what assets they have assigned to them—essentially, a good snapshot of who they are, where they are, what they have."

The rise of multi-tech credentials has made it possible to get this insight while enhancing the overall user experience.

> *You can use multiple technologies on a single card—prox and Seos for instance—depending on what system you're using it with. All the user knows is that they're using their card. The copy machine is using the prox portion, the door is using the Seos portion. The user doesn't have to know and doesn't care.*

—Rob Murphy, CPP, CLSD Security, Risk, and Crisis Strategist

Such views are gaining traction. The survey found 18 percent of FinServ security professionals rated the integration of physical and logical access control as the most impactful technology advancement in access control. This convergence further mitigates risk by creating layers of security from physical perimeters to connected network devices while painting a fuller picture of who is accessing what locations when, as well as the network-based resources in use. This level of detail enables security and IT leaders to more closely manage access based on an employee's role within the enterprise.



of respondents rate the integration of physical and logical access as the most impactful technology advancement in access control

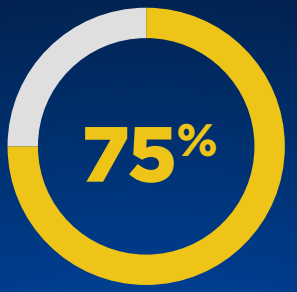
The Benefits of IT and Security Convergence

In order to effectively pursue PACS modernization, FinServ must recognize the intertwined nature of technology and security. A new relationship between IT and physical security professionals is needed to maximize return on the PACS investment while supporting enhanced cybersecurity and protecting PII. Some are moving toward these partnerships. Among FinServ security professionals, 75 percent say they collaborate with IT to establish best practices. But only 53 percent say security and IT seek new technology solutions together, and 19 percent report little to no overlap at all.

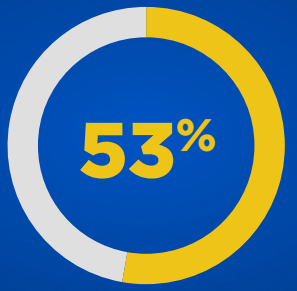
But institutions where IT and security teams collaborate are seeing the value of a close relationship. "Our event logs and history are being analyzed by IT's systems to try to correlate how people are behaving at our bank, and that includes our colleagues," said one security professional. "When someone puts a badge up on a card reader and they don't get access, we need to know how often that happens. They're trying to create these analytics so we can learn how people are behaving."

> *"Our investigations team does a lot of collaboration with our cyber team, and we are in the process of creating physical access relationships with them, too, said one security professional."*
>
> ***—A FinServ Security Professional, Chicago, IL***

Top Ways Security and IT Work Together



Establishing best practices for facility security



Looking for new technologies together

Sharing a budget

Four Practical Steps to PACS Modernization

1 Take Inventory of Existing Systems

It's important to know what components are installed, how long they've been in use, and if the latest version of firmware is installed. PACS managers should survey existing systems, looking especially for insecure technologies, as well as opportunities to consolidate disparate systems onto a common management platform. This effort will support the eventual development of an upgrade plan.

2 Implement Multi-Tech Readers and Credentials

Multi-tech capability enables a path to modernization. Replacing legacy credentials with multi-tech smartcard technology allows for a wide range of applications on a single card. PACS managers should also consider upgrading to mobile-enabled multi-tech readers across the institution to accommodate the variety of credentials in use, as well as any mobile credential deployments.

3 Explore the Use of Mobile

Credentials on a smartphone offer a higher level of security and can reduce the administrative burden in routine areas such as provisioning and lost credentials because people are far less likely to lose a phone than a card. Mobile credentials offer the means to rapidly and effectively deploy and manage credentials in support of both access and identity.

4 Centralize Management

Centralized identity management solutions can help manage identity across multiple business systems, simultaneously easing the administrative burden on under-resourced security personnel. Such centralized management supports the convergence of IT and physical security. This integrated approach offers a means to secure user identities in all environments, with physical access and network access intimately linked and under centralized control.

How HID Can Help

To modernize their PACS deployments, FinServ security professionals need the support of a trusted partner with a deep understanding of the evolving technology landscape.

Every day, millions of people in more than 100 countries use HID Global products and services to securely access physical and digital places. Over 2 billion things that need to be identified, verified and tracked are connected through HID's technology. Financial institutions trust HID and its global network of partners to help create trusted physical and digital environments.

To speak with someone from HID Global about converging your physical and logical access control, contact: **gethid@hidglobal.com**

To learn more about HID Global's range of access control solutions click here. **https://www.hidglobal.com/access-control**

HIDGLOBAL.COM

Learn how your financial institution can create a multi-layered security strategy that protects your buildings, networks, and systems. Visit the HID Global website for more information.

LEARN MORE

hidglobal.com

2021-04-09-pacs-securing-financial-institutions-eb-en PLT-05746

Part of ASSA ABLOY