Brought to you by POINT.CO

Managing Identity:

10 Steps to a Smoother Post-Merger Integration

As today's companies seek to expand and diversify, the number of mergers and acquisitions (M&As) is growing fast. According to a recent Deloitte survey,[1] 79% of corporations expect the number of deals they close to increase in the next 12 months.

While more enterprises plan to make acquisitions, as many as 70–90% of M&As end up failing.[2] One of the reasons? The lack of a clear identity integration process.

M&As require a tremendous amount of planning as the two companies join together. And in addition to deciding which systems to keep and what business functions to integrate, a key component is securely and seamlessly managing the larger pool of user identities that result from the merger.

In recent years, the risk of data breaches during an M&A has been growing. In fact, **44% of organizations say the importance of cybersecurity attacks has significantly increased at target firms during an M&A, while 56% say it's increased somewhat**, according to a Donnelley Financial Solutions survey.[3] Moreover, companies have a lot to consider as they strive to merge while maintaining a seamless customer experience.

Take the example of a media company that extends its reach by acquiring a media company in another region. The two companies have disparate customer-facing websites, mobile apps, and customer relationship management apps, as well as apps and websites for multiple brands. Without a solid plan to seamlessly integrate the identity requirements of both companies, the post-merger brands risk service disruptions that can lead to lost customers. The organization also exposes itself to security and compliance risks.

1. Deloitte, "The state of the deal: M&A trends 2019"
2. KPMG, "Improve your deal results with a new approach to synergies," 2018
3. Donnelly Financial Services, VENUE® ® Market Spotlight CYBERSECURITY, September 2017

Now consider a large tech company that diversifies its offerings by acquiring a specialized cloud solution provider. Figuring out which employees need access to what systems can be a huge undertaking — lengthy delays can lead to costly downtime and even lost talent. And if customer service reps can't access the information they need, the post-merger company's customers may quickly become frustrated and walk away.

Identity is a major concern following an M&A integration. And a concrete plan for securely and seamlessly managing identity and access management (IAM) can make the difference between an acquisition that quickly captures value and one that damages your reputation and your bottom line.

So what should companies consider as they integrate identity management following an M&A? Here are 10 steps to help set you up for success:

1. Create a solid strategy to preserve (or improve) the customer experience.

Today, large corporations spend as much as $1 million annually on password-related support costs, according to Forrester.[4] This expense is the symptom of a larger challenge. A big piece of any post-merger identity strategy is making sure that the details of merging identity remain invisible to end-users. Customers are generally averse to change, so this is the moment you need to plan to preserve or improve the customer experience. As Darren Hakeman, SVP, Analytics & Corp. Development at 8x8, told Forbes, "Unless you're very deliberate and intentional about it, the customer and the customer experience can get lost."[5] And a recent PwC report[6] found that 33% of customers did more business with merged

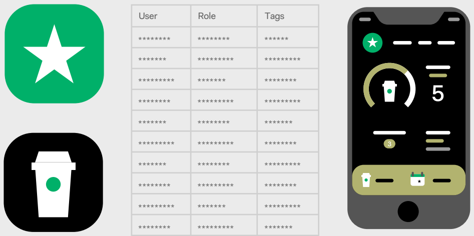
[4] Forrester, "Using Zero Trust To Kill The Employee Password," March 2, 2020

[5] Forbes, "With Mergers And Acquisitions, Customer Experience Is The Key To Success," October 14, 2019

Why Identity is Key for Effective Post-Merger Integration

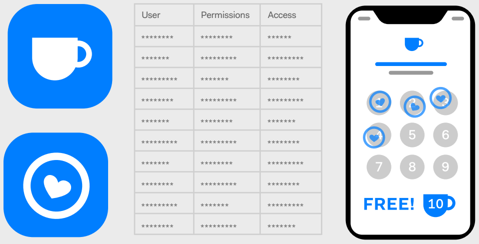
To reduce costs and create a seamless experience for your expanded pool of users, an acquisition means you need to plan to integrate **legacy databases, custom apps,** and **loyalty programs.**

AQUIRING COMPANY



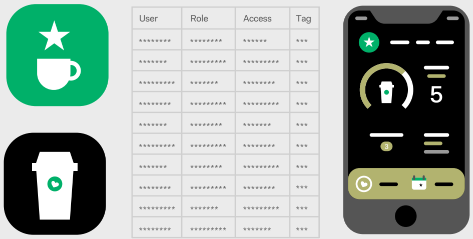
Companies with the resources to acquire other companies often have multiple legacy databases, custom apps, and potentially higher security expectations, as well as fully established loyalty programs.

TARGET COMPANY



Target companies often offer innovative and agile apps, built on newer technologies, as well as customers who may have strong brand loyalties.

RESULTING MERGER



Customers often view loyalty rewards as actual cash in their pockets. A frictionless user experience, with strong brand messaging, can help protect against customer loss during M&A transitions.

44%

of organizations say the importance of cybersecurity attacks has significantly increased at target firms during an M&A[1]

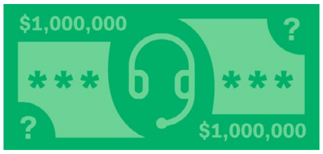
51%

of customers will leave after just one bad customer experience with a company.[2]

70–90%

of mergers and aquisitions end up failing.[3]

1. Donnelly Financial Services, VENUE® ® Market Spotlight CYBERSECURITY, September 2017
2. Vonage, “The $62 Billion Customer Service Scared Away.”
3. KPMG, “Improve your deal results with a new approach to synergies,” 2018



Today, Large corporations spend as much as **$1 million** annually on password-related support costs[4]

companies when they remained through the M&A — a clear indication that keeping customers happy during an M&A matters.

Strategically putting the customer first can reshape how you merge both companies' strengths and resources. When it comes to everything behind the login box, merging companies is a bit like using Android and iPhones — they can both make calls and even swap files, but you need different charging cables and other technical bridges to switch from one to the other.

Creating that strategy may mean blending the approach of a startup who had the luxury of building their identity strategy from scratch with a large mix of legacy resources and applications that stretch across multiple brands. As well as planning for the moment when you might welcome customers to your site with a new logo. Companies often focus their customer communication in the form of social media, press releases, and advertisements, but frictionless login and migration experiences also make a strong brand impression.

[6] PwC, "CX in M&A: What consumers think when companies combine," April 2019

2. Factor in cost avoidance.

As you plan your post-merger IT integration, it's critical to consider where you may take on costs or lose revenue. For example, downtime for merging identity stores or replacing authorization middleware can add up to hundreds of thousands of dollars in lost business.[7] And when users can't access the systems they need or must re-enter their credentials to log in to different systems, the costs can rapidly add up. The situation is similar when customers suddenly become victims of a fragmented experience — say, when they're forced to log in separately to access multiple websites or mobile apps. According to one service, 51% of customers will leave after just one bad customer experience with a company.[8]

While a haphazard approach to the post-merger integration often amounts to lost value, organizations that successfully plan their IT integration can save costs while increasing their value from the acquisition. Anticipating where the costs are likely to add up allows your organization to decide which identity management challenges to tackle first. This detailed cost assessment will help your organization avoid the unexpected losses that can significantly diminish the value of your M&A investment.

3. Think through the both companies' approaches to authorization.

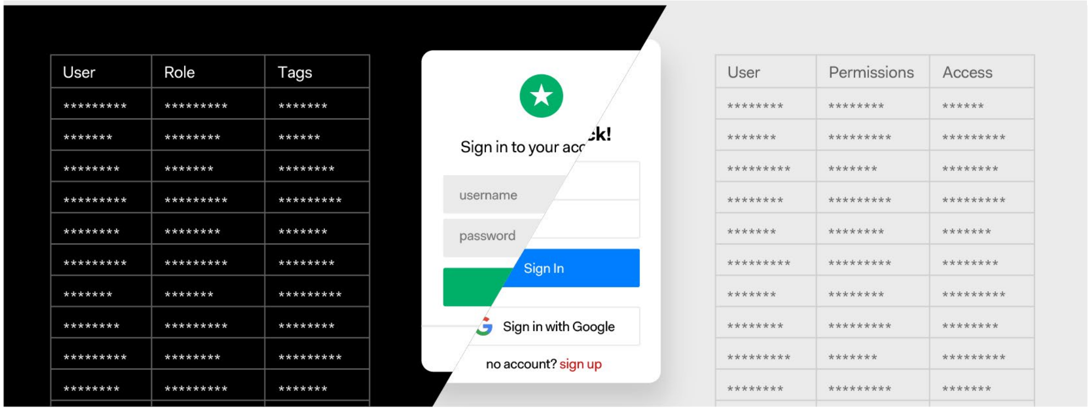
When you merge with another company, the organization you're acquiring may have a very different approach to authentication and authorization. Without an organized plan for determining which users have access

[7] Rand Group, "How Much Does 1 Hour of Downtime Cost the Average Business?"

[8] Vonage, "The $62 Billion Customer Service Scared Away"

to what resources, the result can be chaos, with some users accessing resources they shouldn’t and others being inadvertently locked out.

By taking the time to understand how each company approaches authorization, you can develop consistent authorization policies as you combine systems. The right IAM platform can help you manage this complexity by automating the translation of access rights and metadata, as well as by grouping users into roles based on their common responsibilities and the access they need. By assigning permissions using role-based access control (RBAC), you can quickly match the right users with the right resources across both the parent and acquired company.



Getting the right users the right resources
By assigning permissions using role-based access control (RBAC), you can quickly match the right users with the right resources across both the parent and acquired company.

4. Make sure your apps don’t end up siloed.

To maintain operational efficiency following an M&A, you need to make sure that both employee and customer identities are recognized by each application and resource during and after merging the identity stores. It is not uncommon for one or both company’s applications to use incompatible technologies or be written without adherence to industry standards.

This often leads to a large scale “forklift upgrade” of these systems, where most of the work needs to be done well in advance of any migration or merging of systems. This often leaves employees and customers forced to authenticate directly with the various applications, using separate identities.

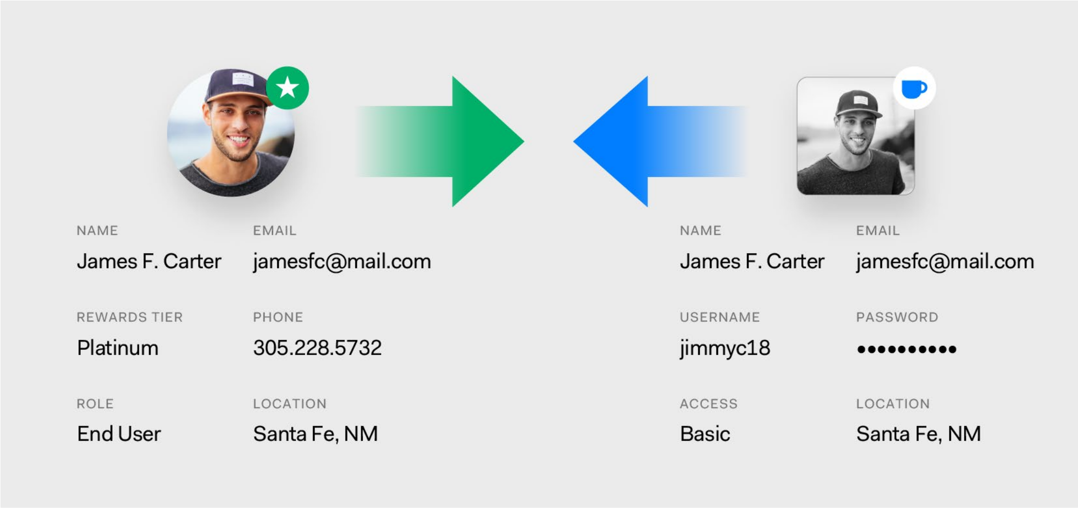
Instead, opt for an identity platform that can consume and merge all of the different identity sources, quickly integrate with all of various applications already in place at both companies, and offers customizable business logic to handle edge cases, while maintaining the merged company’s security, governance, and compliance.

5. Complete your user migration and user consolidation plan.

Consolidating user identities can be one of the most challenging parts of a post-merger IT integration. Typically, each enterprise has identity data stored in multiple directories and databases, including legacy stores that have been customized over time.

Once the two companies merge, IT and Product teams are suddenly faced with siloed and inconsistent information from one source to the next. Integrating these databases can lead to a barrage of password issues that tie up your Help Desk and keep your staff from other projects. Employees may experience gaps in productivity, and customers may have trouble accessing customer-facing applications.

As you implement your user migration plan, you need to consider how to centralize identity management without disrupting the flow of work. Do you plan to combine directories or continue to support them separately?



NAME James F. Carter	EMAIL jamesfc@mail.com
REWARDS TIER Platinum	PHONE 305.228.5732
ROLE End User	LOCATION Santa Fe, NM

NAME James F. Carter	EMAIL jamesfc@mail.com
USERNAME jimmyc18	PASSWORD ●●●●●●●●●●
ACCESS Basic	LOCATION Santa Fe, NM

How will you centralize identity management?
As you implement your user migration plan, you need to consider how to centralize identity management without disrupting the flow of work — or the user experience.

How will you ensure that business can continue while you undertake the merger of the various Enterprise or customer directories? Whatever option you choose, make sure you avoid harming the customer and employee experience with an identity platform that lets you automatically migrate and merge users without requiring them to reset their passwords or disrupting the flow of work.

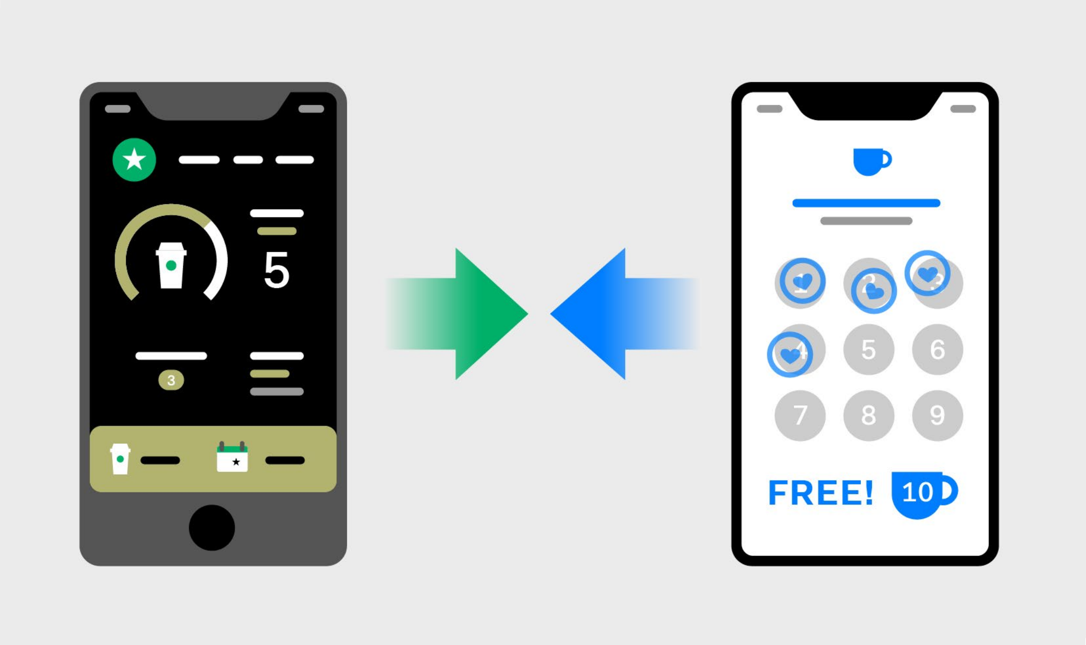
6. Craft your user reconciliation plan.

Another factor to consider as you integrate your acquired company is how you will reconcile user accounts to ensure that data is up-to-date and avoid duplicate user accounts. When a user's log-in information isn't updated or they have duplicate accounts, their information can't easily be accessed, leading to confusion and a poor customer experience. And when two companies merge, the risk of duplicate accounts grows with the parent and target company relying on different directories and identity providers.

Be sure to specify how you will deal with this issue as part of your post-merger IT integration plan. The best way to simplify user reconciliation is with an identity platform that can automatically unify the various accounts of all of your customers and corporate users under a single user record — and then offer the business logic needed to determine how those credentials can be used to access the various resources of both organizations.

7. Create a plan for existing loyalty programs.

When two companies merge, they often have different ways of working with customers, leading to inconsistencies that can undermine hard-earned customer loyalty. According to a Deloitte survey, 19% of corporate and private equity executives say their deals haven't performed as well as expected because the two cultures are misaligned. When the two cultures have different processes and approaches, it often results in a less than optimal customer experience.[9] Only 30% of consumers say they



How will you handle existing loyalty programs?
One way to retain customers following a merger is to carefully consider how you handle existing customer loyalty programs. Do you keep both programs, blend them into one, or let one loyalty program dominate?

believe companies think about how customers are affected during an M&A, according to a PwC survey.[10]

One way to retain customers following a merger is to carefully consider how you handle existing customer loyalty programs. In many cases, each company offers a different customer loyalty program with a different set of goals. Do you keep both programs, blend them into one, or let one loyalty program dominate? Whichever option you choose, how will you explain the change to members who may be attached to their status?

As you weigh your options, one issue to consider is incompatible metadata. If you can't directly import the other company's customers, you may be forced to create a disjointed experience that requires customers to log in separately to each application. Yet with the right IAM solution, you can avoid this problem. By choosing an identity platform that can automatically transform and merge metadata from different identity sources, you can seamlessly merge multiple customer loyalty programs without requiring customers to bear the brunt of the effort.

8. Develop your mobile apps strategy.

Another consideration is how you will manage IAM for your mobile apps. What mobile apps does each company currently offer its customers? And will you be consolidating these apps, maintaining them, or creating entirely new ones? How do they interact with incumbent identity solutions? Regardless of what solution you choose, you'll need to develop a seamless plan for authenticating and authorizing the customers of both companies, with the goal of allowing them to easily authenticate and migrate with minimum friction.

[9] Deloitte, "The state of the deal: M&A trends 2019"

[10] PwC, "CX in M&A: What consumers think when companies combine," April 2019.

One way to achieve that is by offering Single Sign On so users can authenticate once to access multiple applications (including scenarios like federating from a mobile app to a web site). The best IAM solutions offer cutting-edge security and ease of use, the flexibility to use any source of identity, and require minimal code changes in your existing mobile apps.

9. Avoid brand-damaging data privacy missteps.

Data breaches are on the rise, and the probability goes up during an M&A. This can be due to a variety of factors, such as inheriting vulnerabilities, insider threats, or relaxed security while resources are commingled. The Donnelley Financial Solutions survey found that "80% of respondents say that they have uncovered data security breaches in between 26% and 75% M&A targets. Asked about their biggest concerns about an M&A cyberattack, 60% of respondents say they're most worried about potential theft of intellectual property, while 20% cite damage to their company's reputation and 20% cite legal liability.[11]

Marriott learned firsthand the toll a data breach can take after an unauthorized party accessed the reservation database of its acquired company Starwood properties, exposing the personal information of 383 million customers. The incident resulted in a $123 million fine levied by the UK's Information Commissioner's Office[12] as well as multiple consumer class action lawsuits.[13]

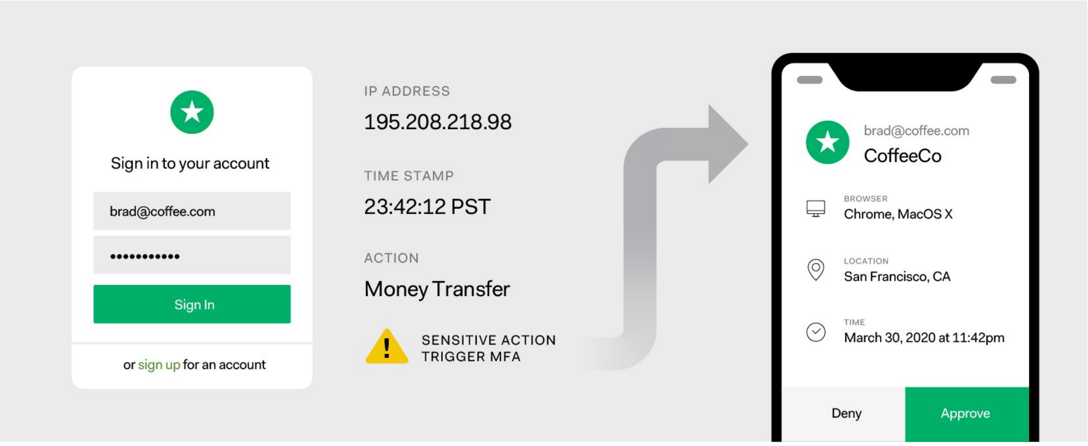
[11] Donnelly Financial Services, VENUE® ® Market Spotlight CYBERSECURITY, September 2017

[12] Forbes, "Marriott faces $123 million GDPR fine for last year's data breach," July 9, 2019, GDPR May Add Up to $915M Marriott's Data Breach Expenses," Jan. 9, 2019.

[13] CNBC, "Marriott breach sparks multibillion-dollar suits, with more to come," Dec. 4, 2018.

As you plan your post-merger integration, it's necessary to understand the data privacy and cybersecurity risks. Has the company you are acquiring experienced past data breaches? How does the company handle sensitive data, and are there vulnerabilities? What existing cyber-relevant contracts does the target company have with vendors and customers? And what cybersecurity and data privacy standards is the company required to adhere to?

As you research the target company's security practices, it's important to remember that identity is ring zero for security. To avoid damaging data breaches, it's critical to choose an IAM solution that adheres to the industry's most stringent security standards. You also want a provider that offers the architectural guidance you need to implement security best practices across your organization, without trying to force you into a "one size fits all."



brad@coffee.com
•••••••••••

IP ADDRESS
195.208.218.98

TIME STAMP
23:42:12 PST

ACTION
Money Transfer

brad@coffee.com
CoffeeCo

BROWSER
Chrome, MacOS X

LOCATION
San Francisco, CA

TIME
March 30, 2020 at 11:42pm

When to Use MFA
You can help balance security and user experience, by requiring end-users to use multi-factor authentication only when triggered by a sensitive action.

10. Protect customers with multi-factor authentication.

As you merge with another company, one way to protect your customers is by requiring multi-factor authentication (MFA). Implementing MFA is always a balancing act between security and user experience. The added layer of security lowers the chances of unauthorized access. Yet requiring more than one piece of identifying information can add the friction of extra steps for your customers.

The answer is to provide MFA only when it's truly necessary. By choosing an IAM solution that offers contextual MFA, you can obtain maximum flexibility as to when MFA is triggered. Perhaps you only want to activate MFA when a user attempts to access a sensitive area of an application, or makes a real-money transaction, or every time a user logs in from a new device or browser, or for customers with certain risk scores, or combination of attributes. Contextual MFA enables you to set up the customized rules that make the most sense for your business — allowing your organization to maximize security when needed while removing the unnecessary obstacles that prevent legitimate customers from having a smooth experience with your company.

Mergers & acquisitions can be complex. Yet with some advance planning and the right IAM platform, you can simplify many of your major identity challenges. With a flexible identity solution that works right out of the box, you can maintain customer loyalty, improve productivity, and avoid hidden costs — helping your organization capture the full value of your M&A investment. To learn more or to talk to an identity resource, visit Auth0.com.

Point is a national IT firm specializing in Identity, Endpoints and Cloud Infrastructure. Visit POINT.CO for more info.

About Auth0

Auth0 is the first identity management platform for application builders, and the only identity solution needed for custom-built applications. With a mission to secure the world's identities so innovators can innovate, Auth0 provides the simplicity, extensibility, and expertise to scale and protect identities in any application for any audience. Auth0 secures more than 100 million logins each day, giving enterprises the confidence to deliver trusted and elegant digital experiences to their customers around the world.

For more information, visit https://auth0.com or follow @auth0 on Twitter.