White Paper

Mitigate Cyber Risk while Increasing Deal Velocity for Financial Services M&A

Introduction

Zscaler's comprehensive cloud-native platform securely connects everything, simplifies user experience and onboarding, and lowers deployment and operational burden while comprehensively protecting assets from cyber threats so the business can do M&A/D transactions with higher volume, velocity, and confidence.

Challenges for M&A/D in financial services

The banking, financial services, and insurance (BFSI) sector is witnessing wide ranging changes that are disrupting their business models, and, in some cases, threatening their very existence. Low-interest rates, regulatory oversight, and uncertain monetary policy combined with massive digital transformation-induced changes, such as decentralized finance and FinTech, have made organizations in the BFSI sector prioritize inorganic growth strategies, especially in cases where their technological capabilities are lagging.

Fintechs with mature business models are becoming increasingly active in transactions. Eight categories of transactions are emerging, including the following:

1. Digital banking (e.g., MoneyLion's acquisition of EVEN for $440 million)
2. Payments (e.g., Mastercard's acquisition of nets for $3.2 billion)
3. Buy Now Pay Later (BNPL) (e.g., Square's acquisition of afterpay for $29 billion)
4. Lending (e.g., Rocket Companies' acquisition of Truebill for $1.3 billion)
5. Wealth management (e.g., J.P.Morgan Chase's acquisition of Nutmeg)
6. Insurance (e.g., Lemonade's acquisition of metromile for $500 million)
7. Fintech platform (e.g., Visa's acquisition of tink for $2.2 billion)
8. Decentralized finance (e.g., Gemini's acquisition of blockrize)
9. Regional bank consolidation (e.g., Old National Bank's acquisition of First Midwest for $2.5 billion)

The deal thesis for the above transactions appear to be:

1. A large incumbent BFSI organization acquiring a Fintech for technology-driven platform capability (e.g., proprietary algorithm, data science models)
2. A growing Fintech acquiring another Fintech to consolidate leadership position

For the M&A activity to yield the expected results, deal makers and executives should proactively address areas that can adversely affect the estimated valuation and synergies.

Imbalance in technology stack

Organizations in the BFSI sector have developed a complex mix of technology systems over the past two decades, leading to significant technical debt. Many organizations have adopted digital technologies with little thought to accruing technical and functional debt. This can result in significant risk during M&A situations because it becomes difficult to assess the merging organization's risk posture. As a result, organizations never achieve the estimated revenue and cost synergies.

The information security policies at large organizations established for a traditional network perimeter–based security architecture may not apply to Fintechs that are born in the cloud. For example, a large North American financial institution operating on a castle and moat security architecture (e.g., firewalls, VPN) has struggled to integrate the cloud native tech platform from its Fintech acquisitions, resulting in poor end-user experience.

Cybersecurity and data vulnerability threats

Cybersecurity and data vulnerability issues often arise after the announcement of any inorganic transaction, as bad actors look to capitalize during this ambiguous time of transition, when employees are especially vulnerable. In BFSI organizations, the demand to rapidly secure regulated data, processes, and the ecosystems of sites and partners is paramount to remain both compliant and out of unfavorable headlines. Additionally, lack of a thorough due-diligence process to understand the risk posture of acquired companies can become a regulatory nightmare for companies in this sector. For example, PayPal had to suspend the services of TIO Networks nine months after its acquisition because of a massive breach that was not detected and reported in time.

According to a report released by Kroll, 13% of all cyber attacks are focused on the BFSI sector, which include ransomware, social engineering and business email compromise.

Zscaler helps M&A integrations run safer and faster

Zscaler delivers a modern approach to M&A/D integrations and separations, based on the concept of a Zero Trust Exchange delivered in an as-a-service, pure cloud platform. The Zscaler Zero Trust Exchange securely connects users to systems, applications, devices and each other without connecting any of it to the acquiring or separating company's network. The platform delivers instant access to data and ensures uptime, while protecting the firm's network against potential cyber risks and threats. The result is a highly scalable, safe, and transparent integration sandbox that can be reused time and again.

Realize time to value in weeks vs. months & quarters

Zscaler simplifies the integration process with its cloud-delivered Zero Trust Exchange to near-instantaneously streamline network architectures and security standardization across the environment. Businesses leveraging Zscaler can integrate as much or as little as they need versus defaulting to integrating everything or being bound in some way (time, performance, cost, experience) by traditional M&A technology complexities.. The as-a-service delivery of the Zero Trust Exchange produces a network and security future state on Day 1. Fully operational in days, Zscaler removes barriers to action, allowing organizations to value-capture synergies sooner.

Mitigate and control risks with a common security policy
Zscaler actively protects the enterprise from known and evolving cyber threats and insider risk with a simple-to-operate, scalable cloud platform. Because all traffic can run through our platform, organizations can shift their focus from protecting their perimeter to protecting their traffic. Zscaler provides detailed visibility and auditability to all access across the enterprise in a single control plane, while identifying and mitigating all network-born threats.

Simplify integration and optimize costs by administering, not engineering
The platform enables IT/Security operations to securely connect any device, application, or user no matter where they work, travel to, or connect from. All access is granted near-effortlessly. Through business logic policies organizations can securely control, connect, and audit applications, users, and workloads access without the need for a private network or an SD-WAN. Moreover, enterprises can leverage the power of the internet and the largest global secure data exchange to transport corporate traffic, and seamlessly scale on-demand with growth and acquisitions, or with a user- /consumption-based model. There are no hardware limits or capacities to self-manage.

Increase business agility and flexibility
Because Zscaler eliminates many time-consuming and complex technical integration components, the platform helps turn M&A transactions into highly repeatable processes. Zscaler simplifies the integration by enabling administrators to pick and choose which systems are needed and can help separate divested assets without the 'clone and go' approach.

How the Zscaler Zero Trust Exchange securely accelerates M&A/D transactions

The Zero Trust Exchange is the core of the Zscaler platform, enabling businesses to securely accelerate their digital transformation. The Exchange expands IT environments so employees can work from anywhere, while maintaining a comprehensive security standard. It allows increased connectivity and decouples security from the network.

Simplify network transformations
The Exchange moves from a hub-and-spoke approach to a direct-to-cloud model. It's a modern and simplified approach that removes most difficulties associated with network integrations, hardware, and address space. It provides a single control plane for any cloud strategy—hybrid, multi-cloud, multi-tenant, multi-VPC strategy—and allows direct application access for any program hosted anywhere.

Transform and modernize security
The traditional castle-and-moat perimeter approach is being phased out in favor of the zero trust model. Zero trust provides a secure and direct connection that reduces potential vulnerabilities for storage and moving data—in SaaS and public clouds—and applies to almost any type of security threat. With Zscaler, threats can be limited in their ability to move laterally, and the platform's scalability reacts to new and evolving threats in near real-time.

Enable the modern and mobile workforce

Today's workforce is mobile and decoupled from physical spaces. The Zero Trust Exchange supports this by giving policy-based access to users wherever they are, regardless of location. Gone are the days of tunneling into networks, and issues are proactively resolved with a shift-left strategy. The platform can be scaled to meet new user demands, wherever or however they access the internet.

Zscaler is the modern way to integrate

The immediate ability to share processes and data without disruption from anywhere is a compelling differentiator Zscaler brings into BFSI M&A. Zscaler's simplicity gets integrations done in far less time, and does so with little user disruption. Zscaler allows organizations to quickly begin value-capture activities while increasing the volume of inorganic transactions. Contact us for a demo today.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com