Authentication Security in Financial Services in the UK: Moving Beyond Compliance

At a Glance

For UK Financial Services Organizations:

63%
Had an authentication-related breach

$1.71 Million
Cost of an authentication-related breach annually

68%
Kept their insecure authentication even after a breach

Introduction

The United Kingdom has consistently taken a strong position on cybersecurity, recognising the need to drive awareness and responsiveness on a national scale. It established the National Cybersecurity Centre in 2016, has among the strictest security and data protection laws, and recently launched its £2.6 billion National Cyber Strategy. The tough stance holds even more true for banking and financial services organisations, with additional requirements imposed by the Bank of England's Prudential Regulation Authority (PRA) and international bodies, such as PCI-DSS.

Challenges of Compliance-Driven Security

While these regulations are positive steps, it means compliance ends up driving many security decisions — to the potential detriment of organisations and their customers. In a recent Ernst & Young survey, CISOs in the UK named ensuring compliance as the most stressful element for their role, yet only 36% believe that compliance requirements focus on the right aspects of security.[1]

In fact, compliance requirements typically lag far behind current attack landscape risks. Nowhere is this more evident than in authentication security.

HYPR and Vanson Bourne recently conducted a survey on the authentication practices and security of financial services organisations in the UK as well as the US and Europe.[2] Results show the repercussions of over-relying on regulations to drive cybersecurity infrastructure decisions.

[1] *https://www.ey.com/en_uk/consulting/ey-uk-global-information-security-survey-2021*

[2] *Technology research firm Vanson Bourne interviewed 100 IT security DM respondentsfrom UK organisations in the financial services sector, along with respondents in the US,France and Germany, during April-May, 2022*

Attacks and Breaches

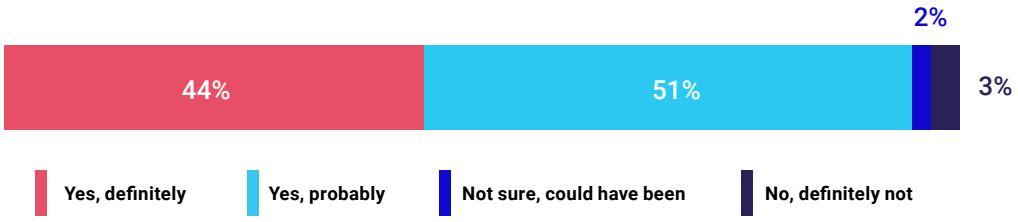
Let's start with the good. Overall, UK financial services organisations report significantly fewer cyberattacks than other regions. A full 18% say they haven't faced any cyberattacks in the last 12 months whereas the average rate is 6%. Moreover, those attacks are less likely to lead to a breach, at 80% for UK firms versus an average of 90%.

However, this still means that a full two-thirds of all UK financial organisations have been breached. In fact, most have been breached multiple times, to the tune of 3.1 breaches annually, on average.

Authentication Vulnerabilities Causing Breaches for UK Financial Firms

Moreover, the positive comparison ends when it comes to authentication-related breaches. Looking at root causes, 95% of organisations that were breached named credential misuse or authentication vulnerabilities as a factor in at least one breach. This data indicates that authentication remains the biggest point of weakness for financial organisations in the UK; regulations are simply not enough.

Question: Were any of the cyber-breaches that your organization experienced related to credential misuse or authentication vulnerabilities?



Note: Only asked to respondents whose organisations have been the victim of a cyber-breach as a result of a cyber attack in the past 12 months

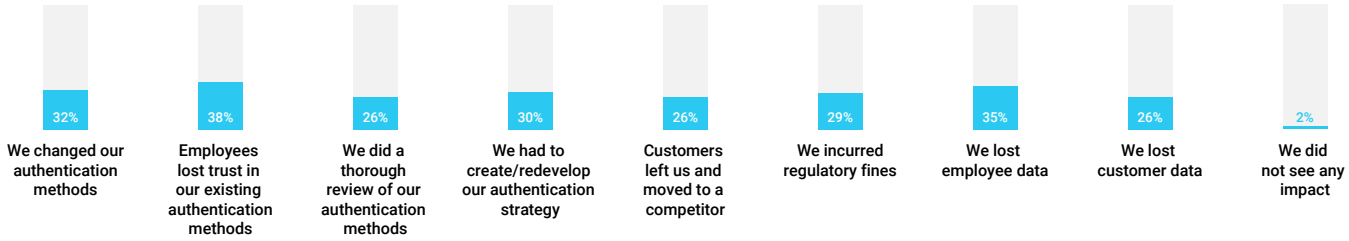
Impact on Business and Customers

There's no point in mincing words. The current authentication practices of financial services organisations in the UK is causing harm to their business and their customers. Authentication-related breaches cost UK firms an average of $1.71 million annually and led to other significant consequences including loss of business (26%), fines (30%), loss of customer data (26%) and loss of employee data (26%).

Moreover, despite the negative impact, only 32% of organisations in the UK changed their authentication practices after a breach. Compare this to the U.S. where 44% took action.

In other words, 68% of the financial firms that were breached are still vulnerable.

Question: What was the impact of the cyber breach(es) that your organisation experienced in the last 12 months?



Note: Only asked to respondents whose organisations have been the victim of a cyber-breach as a result of a cyber attack in the past 12 months

Few Heeding the Wake Up Call

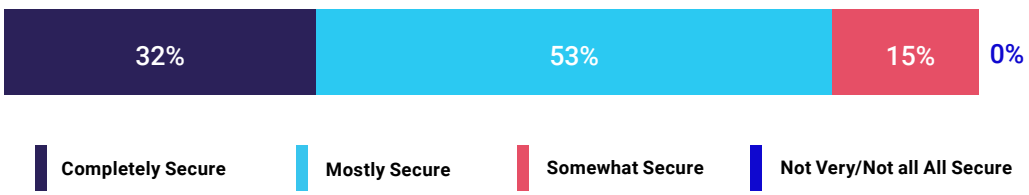
Digging in deeper, we see evidence of persistent insecure practices when it comes to authentication and a strong suggestion that compliance-driven security may play a role.

While UK organisations deserve credit for doing a good job on the most egregious bad practices — for example, UK firms are 23% less likely than their global counterparts to authenticate with only a username and password (17% vs. 22%) — these seem to have been replaced by only marginally more secure authentication methods. Fully half of UK financial firms employ insecure 2FA technologies such as SMS and OTPs, compared to 32% globally.

The numbers make sense when you consider that regulations currently on the books mandate MFA, but do not distinguish between phishing-resistant passwordless MFA and legacy methods. If the last few years have taught us anything, it's that standard MFA authentication methods offer little protection against modern attacks.

This mis-alignment clearly creates a false sense of security for many UK financial organisations as 85% state they believe their authentication approach is secure, despite the large number of breaches.

Question: How secure do you consider your organisation's approach to authentication to be?



Conclusion

These findings reveal the repercussions of focusing on compliance rather than the critical security risks facing UK financial organisations. Regulations are not enough to keep authentication-related breaches in check, directly costing these organisations over $1.7 million a year.

All organisations, but the finance industry in particular, need to contend with a dynamic threat landscape and evolving business and operating environments. Industry research indicates that most CISOs and IT leaders would rather build cybersecurity structures for the critical risks that their organisations face, rather than simply to align with compliance requirements.

These risks aren't only security-related. Cybersecurity initiatives need to address the commercial needs of the business and act as strategic enablers, rather than obstacles to change. Ticking off a compliance checkbox on multi-factor authentication won't cut it.

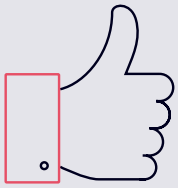
Newer phishing-resistant, passwordless technologies offer a clear path forward for UK financial firms to remain both secure and competitive. The survey found that the vast majority of Security & IT decision makers at these firms (81%) believe passwordless authentication ensures the highest security. Even more, (89%) state that passwordless authentication improves user experience.

It's Time To Go Passwordless

HYPR True Passwordless™ MFA provides phishing-resistant security that financial services organisations require while making the authentication process fast and frictionless for users. Designed to deploy rapidly into existing infrastructure, it turns an ordinary smartphone or other device into a PKI-backed security key. In a single, secure authentication gesture, users gain seamless access to their desktop device and all downstream local and cloud-based applications. HYPR is deployed and battle-tested in some of the largest banking and financial institutions in the world, with 3 of the top 4 banks HYPR customers.

81%

state that passwordless authentication provides the **highest level of authentication security**



89%

report that organizations need to fully embrace passwordless authentication to **ensure user satisfaction**

THE PASSWORDLESS COMPANY

Email: info@hypr.com
Learn more: www.hypr.com

HYPR fixes the way the world logs in. HYPR's true passwordless multi-factor authentication (PMFA) platform eliminates the traditional trade-off between uncompromising assurance and a consumer-grade experience so that organizations decrease risk, improve user experience and lower operational costs.