Securing payments innovation

Reshaping the banking experience

For a time, banks were the kings of payments. Throughout the debit card era and well into the digital era, banks held a virtual monopoly over the payments ecosystem.

No more. Over the past few years, we have seen the rise of a range of new payment service providers. Some, like PayPal or Apple Pay, have created massive 'merchant' networks through their online presence and partnerships with some of the bigger platform players. Others have found niches in their own areas, often responding to specific customer pain points in the payment environment.

Not surprisingly, many of the world's leading banks are now working closely with these payment service providers to create solutions and tools that both respond to shifting customer demand and keep the bank in the value chain. Exciting new innovations and models are emerging.

Risk grows exponentially

Innovation in the payments sector is critical. Partnerships with third parties is a key strategy for achieving the type of innovation required in today's rapidly-changing environment. However, this also creates increased risks.

For all intents and purposes, the term 'third-party risk' has long become a bit of a euphemism in the payments world: many of the better-integrated payment service providers are now so connected into their banking partners' enterprises that there is often little difference between a bank's payment systems and employees and those of their 'third-party' payment providers.

Yet it is exactly this embeddedness that makes partnerships with third-party payment providers seem so beguilingly secure. The assumption is that their employees are following the same protocols, using the same controls and taking the same precautions as the banks' own employees. Yet, often they are not.

The leading banks are therefore placing increased focus on managing these third-party relationships, closely integrating and overseeing their service providers in a way that allow them to become an extension of the banks' own lines of business.

What's the trade-off?

It will take more than increased oversight and control to make a new payment innovation succeed. It will also require the highest levels of security. And that means that bank and payment executives will need to ensure their drive towards innovation remains focused on delivering customer convenience and security.

The problem is that proactive investments in security rarely move the meter with customers. They see security — cyber or otherwise — as table stakes in a payment transaction; keeping their money and data secure is a given. But they also want convenience. They want to rid themselves of two-factor authentications. They want to replace their debit and credit cards with phones and watches. And they want to allow other third parties, of their choosing, to have access to their payment (and even banking) data.

The challenge for banks and payment providers, therefore, is to create partnerships and shared cultures that allow them to respond quickly to customer trends without ever losing sight of their security responsibilities. At every step, the partnership should be asking itself two questions: How does this action improve the customer experience? And how does it impact security?

Divided we fall

Unfortunately, in payments and in the wider digital world, there are no silver bullets that guarantee security. Rather, it requires a range of strategies, tools and capabilities — all working together — and focused on the risks that matter most to your organization and your customers. It also requires unprecedented collaboration across the ecosystem.

Thankfully, we are seeing good progress and reason for optimism. At conferences like Sibos, banking and payment leaders are coming together to share ideas and strategies for improving security in this type of hyper-connected world. Industry associations and cyber groups are shining the spotlight on some of

the challenges and encouraging collaboration. Even government agencies and spy networks are trying to play a convening role.

Some of the more institutional payment service providers are also taking smart steps to help secure the payment ecosystem. SWIFT, for example, has been fairly active in rolling out solutions — customer security programs, standardized know-your-customer (KYC) data tools and a KYC registry, for example — that at the very least bring standardization and a common language to the discussion.

But more collaboration will be required. The reality is that this is not an issue that can be tackled or solved alone. In fact, those who do decide to 'go it alone' are often the ones most in danger. Rather, it is by sharing our ideas, experiences, threat assessments and tools that we will form a solid defense against cyber threats in a hyper-connected world.

Get ahead of it

While talking, sharing and collaborating is important, so is action. And our view suggests that banks, payment providers and others in the ecosystem could be making a more concerted effort to build security into their products, services and operating models.

One way to do this is to embed cyber into the very early stages of any new business or group strategy. Fraud and risk professionals should almost certainly be included in discussions at the planning and conceptual phases. The bank's cyber professionals should be involved at every step — from conception through development, delivery and beyond.

Just as it is important to embed cybersecurity principles and concepts into the broader organization; in today's hyper-connected world, every employee and third party should understand and actively engage in the organization's cyber strategy. Education and continuous communication with employees is key.

The bottom line here is that banks and payment providers will need to step up their risk controls, models and capabilities in order to deliver what customers want from their payment providers: more convenience with no loss of security.

Attending Sibos this year in London, 23–26 September? Please visit us at booth V105.

About the authors

Chris Hadorn
KPMG in the US
T: +1 404 979 2317
E: chrishadorn@kpmg.com

With over 20 years of financial services experience, Chris leads KPMG's Global Payments team, which collaborates and partners with clients to support their payments transformation needs, including real-time payments and cross-border interoperability.

Natalie Fedyuk
KPMG in the US
T: +1 617 988 5609
E: nfedyuk@kpmg.com

Natalie is a Director in KPMG's Advisory Practice with over 15 years of industry and risk consulting experience helping global financial and healthcare/life sciences companies implement or enhance their cybersecurity, third-party management, and privacy programs. Natalie's expertise spans across multiple disciplines with primary focus on regulatory and technical compliance.

David Hicks
KPMG in the UK
T: +44 20 7694 2915
E: david.hicks@kpmg.co.uk

As KPMG Internationals' Global Forensic Leader, David has significant experience advising firms on financial crime, contentious regulatory matters, bribery and corruption and fraud investigations. David specializes in the financial services sector advising global banks, asset managers and insurers.

For more trends that are reshaping the banking experience, visit home.kpmg/reshapebanking

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Securing payments innovation | Publication number: 136506-G | Publication date: September 2019