



## Captain API

by [Steve Brown](#)

Those of you into superhero lore are undoubtedly familiar with Captain America's primary weapon - his virtually indestructible red, white and blue shield. The shield has abundant aerodynamic properties, and the Marvel comic icon uses it both offensively and defensively. In a recent effort to breathe life into fiction, a YouTube enthusiast known as the Hacksmith constructed his own version of the shield using highly powerful electromagnets. Believe it or not, his replica is reportedly a technological success that is capable of lifting more than 3,000 pounds.

If you've been paying attention to the Fintech space lately, or even if you haven't, the term API may have crossed your desk. If the very sound of it makes you want to raise your techie shield, fear not. We're here to rescue you from any confusion.

For starters, API stands for Application Programming Interface. In laymen's terms, APIs are sets of requirements that dictate how one application can talk to another. Quite simply, APIs make it possible to move information between programs. They're how developers can create new apps that tap into social networks like Facebook or connect to services like Amazon, Google Maps and Dropbox, to name a few.

There are also different kinds of APIs. We bring all this up because here in America, Captains of the financial industry are moving quickly to open up their APIs to third party developers. Changes in European law in fact, mean that within 2Ys, banks in member countries will have to open up access to their payments capabilities, and provide services that will enable their customers to receive data over the internet. This will all be required in a safe, easy and secure way as banks share with third parties.

With these new changes occurring in countries across the Atlantic Ocean, it's not surprising that banks in the EU are therefore taking the lead on open API initiatives. The UK established the Open Banking Working Group last year to explore ways to meet new government standards and to propel banks into the modern era. The result of this working group was a set of standards to guide how open banking data should be created, shared and used by owners and those who access it.

In the US, banks are moving at a slower pace. This is part for competitive reasons and part because of perhaps a fear of the unknown or hacking. Nonetheless, some larger banks including Citigroup, Bank of America, Capital One and PNC have been making pieces of their internally developed software code available to outsiders. This action and the opening up overseas have driven interest from other banks as well.

The good news is that banks stand to profit from API's directly or through licensing agreements with third-parties. They can also use APIs to create more innovative services that will increase customer interaction with the bank. By opening up APIs to third parties, banks can create new revenue streams based on customer-wish lists for products and services that would take too long to build one by one inside the bank itself.

Of course banks have to be choosy about what software and services they allow third parties to access. While banks control precisely what information gets shared, the risk of what can come through the window once it is open is real and worrisome to many technology experts.

The other good news here is that APIs provide narrow, well-defined access to data. APIs don't give anyone and everyone access to internal systems. Even so, everything has to be secured and carefully monitored, so this is not a hassle-free proposition. After all, many banks remain encumbered by a patchwork of outdated and inefficient legacy applications.

For community banks, it is time to begin reading and learning about what APIs are, and how they can help or hinder your business. Here, many banks are just starting to lower their shields to investigate. As you begin, we urge you to explore this opportunity as bankers seek to turn technological fantasy into reality.

# BANK NEWS

## **M&A Activity**

1) United Community Bank (\$1.8B, IL) will acquire Illini Bank (\$282mm, IL) for an undisclosed sum.

## **Payments Biz**

JPMorgan, Bank of America and US Bank will now offer real time payments transfers (peer to peer) to customers through the bank owned platform called clearXchange. The move positions banks against rivals like PayPal.

## **Data Breaches**

Research by IBM Security and the Ponemon Institute finds the average cost of a data breach has now climbed to \$4mm - a 30% increase over the past 3Ys. The study also found that the average time to identify a breach was 201 days and the average time to contain it was 70 days.

## **Less Loyal**

A study by FICO finds 29% of Millennials will leave their bank if they have a single fraud incident (identity theft, lost or stolen information, ATM skimming, or a compromised account). Meanwhile, 25% said they would go to social media and make negative comments if the fraud incident wasn't handled well.

## **Attacked**

The Fed reports it has been attacked by hackers repeatedly since at least 2011. A just released report indicates there were 59 attacks labeled as "unauthorized access" and 55 were flagged as "information disclosure".

*Copyright 2018 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.*