DEC 05
Jenna McNamee

As banks increasingly fall victim to fraud, their weak controls put customers at risk

Article

What's happening? Banks are coming under fire for weak security controls which are leaving consumers more vulnerable to spoofs, scams, and hackers.

The State of the Internet report from cloud service and security provider Akamai Technologies warned financial institutions (FIs) that as open banking begins to proliferate in the US, they must take application programming interface (API) security more seriously.

Elsewhere, UK banks aren't taking full advantage of resources that can prevent their customers from falling victim to authorized push payment (APP) fraud, per FinExtra.

Fraud in the US: According to the Akamai report, as US banks increasingly work with third-party fintech providers via API connections, their API security is weakening or not keeping up with scammers' tactics.

- Within the past year, **attacks on financial-services-related APIs and closely related web applications grew 257%**.
- In North America, the growth in attacks was even higher, at 449%.
- The methods by which hackers use APIs to access personal financial data are becoming more complex, too. If an API is misconfigured, bad actors don't even need a password or login information to access consumer data. Hackers can also gain access directly to files on a bank server through an improperly secured vendor that works with the bank.

APIs power open banking: In partnering with fintechs, banks rely heavily on APIs to create quick and easy connections with third-party providers. The practice is common in the UK, where open banking is part of a national mandate. US banks aren't yet required to implement open banking solutions, though requirements are likely coming.

But many US banks have already felt the pressure from consumers to engage in these partnerships.

US Banks' Deployment of Emerging Technologies, 2018-2022

% of respondents

	2018	2019	2020	2021	2022
Cloud computing	-	-	32%	40%	47%
APIs	-	-	21%	30%	36%
Robotic process automation (RPA)	4%	6%	6%	14%	24%
Chatbots	3%	2%	3%	8%	15%
Machine learning	-	2%	7%	7%	11%

Note: banks that deployed technology going into 2018 to 2022

Source: Cornerstone Advisors, "What's Going On in Banking 2022," Jan 25, 2022

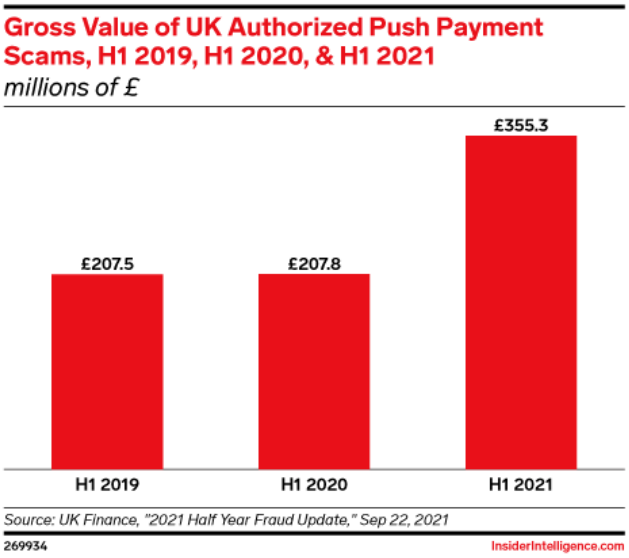
273076 InsiderIntelligence.com

Fraud in the UK: Consumer banking industry group Which? is sounding the alarm against UK banks, claiming many are not fully utilizing the resources available to them to protect consumers from the rampant APP fraud in the country.

- In an effort to prevent APP fraud, the Office of Communications (Ofcom) worked with telecom providers to create a "do not originate" list. This is a list of telephone numbers associated with well-known companies that are only able to receive calls, but cannot place outgoing calls.
- One use of the list is for banks to provide customer service phone numbers on debit and credit cards that consumers can call, but the bank will never use to contact a customer.
- The industry group tested 14 banks' customer service numbers to see if it could mimic an outgoing call from those numbers, or if they were protected by the list. The group found that **it could hack numbers from six major banks**, including **HSBC, LLoyds,** and **Santander**.

APP fraud is fraught: The acceleration of APP fraud in the UK has caused industry groups to label the scam an epidemic.

- APP fraud amounted to £583 million ($686 million) in losses in 2021, an increase of 39% YoY, according to a report from UK Finance.
- And of the total £1.3 billion ($1.5 billion) lost to fraud in the UK, 44% was made up of APP scams.
- In September, the UK's Payment Systems Regulator (PSR) proposed a requirement for banks to reimburse APP fraud victims within 48 hours of the incident. In 2021, APP fraud victims recovered only 47% of losses.



The big takeaway: Innovative technology and financial solutions have revolutionized the industry, providing consumers with countless resources for improving their financial health. But fraud is an inevitable part of tech development, and it's bound to worsen and become increasingly sophisticated. It's imperative that banks, fintechs, and other financial institutions work together to strengthen security controls and prevent scams before they happen.

*This article originally appeared in Insider Intelligence's **Banking Innovation Briefing**—a daily recap of top stories reshaping the banking industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.*

- *Are you a client? Click here to subscribe.*
- *Want to learn more about how you can benefit from our expert analysis? Click here.*