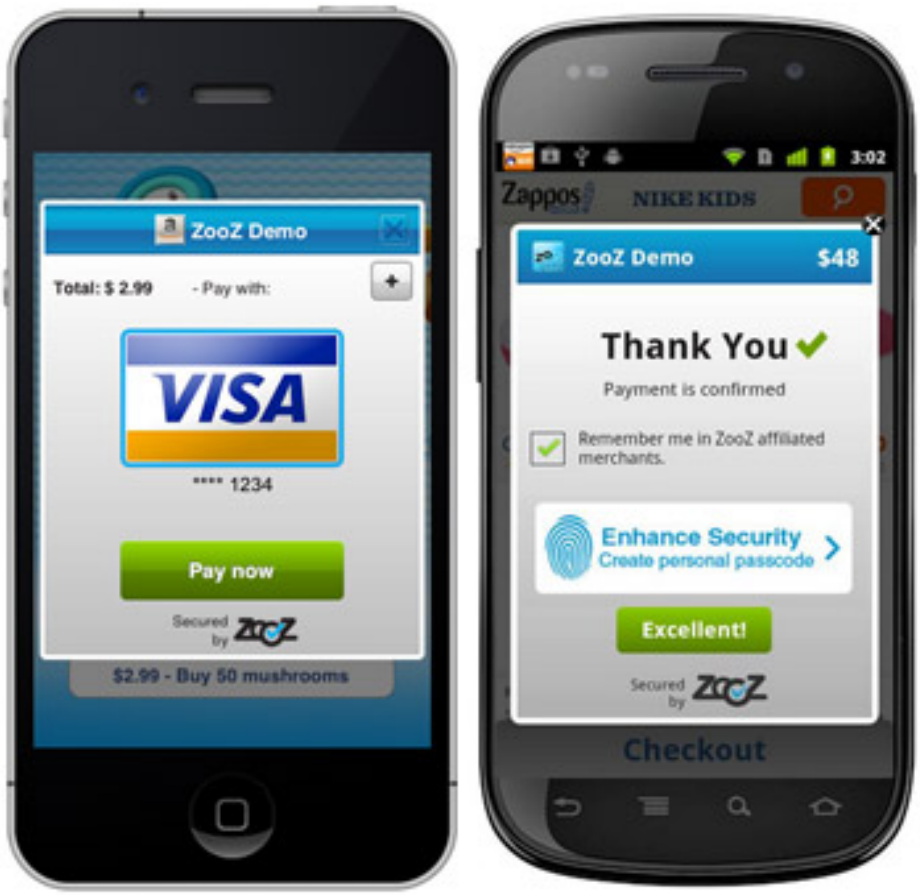
CPA
Practice Advisor

ADVISORY

How Vulnerable Are Mobile Payment Apps to Hacking?

These days, cash and credit cards aren't the necessities they once were because alternative-payment options are just a tap or two away on a mobile device through apps such as Google Wallet, Apple Pay, Square, Levelup, Kash and PayPal.

Sep. 22, 2015



Making a purchase or other payment is not like it used to be.

These days, cash and credit cards aren't the necessities they once were because alternative-payment options are just a tap or two away on a mobile device through apps such as Google Wallet, Apple Pay, Square, Levelup, Kash and PayPal.

But just how secure are those mobile-payment apps and who makes sure that the companies behind them are doing all they can to keep your personal data safe?

The Clearing House, an advocacy group owned by the world's largest commercial banks, is raising those questions and others in a new report titled "Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers."

The report argues that while these providers, operated by both established companies and start-up firms, are subject to some data-security requirements, they don't face the more extensive regulatory oversight banks do when it comes to cybersecurity. That makes it easer for security flaws to go undetected until a breach actually happens.

The Clearing House report raises legitimate concerns, says Gary Miliefsky, CEO of SnoopWall (www.snoopwall.com), a company that specializes in cybersecurity.

"These alternative-payment methods certainly are providing something that consumers want, which is a convenient way to make payments," Miliefsky says. "But I don't think most of those consumers would be too thrilled to know that these companies might not be subject to the same demanding data-security requirements their banks deal with."

It's serious business when companies don't do enough to protect their customers' data, Miliefsky says. Waiting to act after a breach happens is too late because at that point customers are at risk of becoming victims of fraud or identity theft.

"Unfortunately, a lot of companies don't realize just how vulnerable their apps are and what the potential is for leaking their customers' personal information," Miliefsky says.

In its report, the Clearing House made several recommendations and observations, including these related to legislation that would establish additional data-security requirements for alternative-payment providers:

- **Data Security Act of 2015.** This proposed law would establish flexible and common-sense standards for firms of all sizes to follow in order to secure consumers' sensitive financial information and prevent breaches. The law would also give the Federal Trade Commission express enforcement authority in this area, while making clear that the standards are not applicable to financial institutions already subject to similar requirements from banking regulators.
- **More resources.** To exercise any new authority successfully, the FTC would need more resources to properly staff investigations and enforcement actions, the report said.
- **Better security.** Additional legislation might make it clear that alternative-payment providers are subject to the same type of scrutiny with respect to data security as banks. That could be done by directly giving the FTC or the Consumer Financial Protection Bureau examination authority, or by directly requiring the CFPB to enact rules defining larger participants in the alternative-payment industry.

If they aren't already, and regardless of any proposed legislation, the alternative-payment providers should look into better ways to protect their mobile apps from hackers intent on doing harm, Miliefsky says.

There are several ways to do that. Miliefsky's company, for example, offers the AppShield SDK, which can secure any mobile app on all major platforms.

"What the AppShield SDK basically does is make your company's app invisible to any other app on the mobile device that otherwise might be able to eavesdrop on it," Miliefsky says. "I liken it to the way a B2 bomber employs stealth technology to evade radar detection."

Failing to act isn't good for the customers – and ultimately the business, Miliefsky says.

"These alternative-payment apps are a great convenience," he says. "But if they aren't secure, the result could be a huge inconvenience for their users."

————-

Gary S. Miliefsky is CEO of SnoopWall (www.snoopwall.com) and the inventor of SnoopWall spyware-blocking technology. His company produces AppCrusher, which gives companies a detailed analysis of any vulnerabilities or risks in their mobile apps. Miliefsky is a founding member of the U.S. Department of Homeland Security and serves on the

advisory board of MITRE on the CVE Program, and is a founding board member of the National Information Security Group. He's also the original inventor of the NetBeat NAC product line which was recently acquired by SnoopWall to protect networks from the inside and against bring your own device (BYOD) mobile threats.

Advisory • Human Resources & Payroll • Payroll • Product & Service Guide • Technology • News • Hacking • Mobile • Mobile Accounting • mobile banking • Mobile Computing • mobile payments • mobile solutions

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.