Issue: Fintech

Short Article: Fintech Firms' Cyberdefenses Seen as Underdeveloped

By: Victoria Finkle

Pub. Date: September 12, 2016
Access Date: December 12, 2024
DOI: 10.1177/237455680218.n6
Source URL: https://businessresearcher.sagepub.com/sbr-1775-100731-2748722/20160912/short-article-fintech-firms-cyberdefenses-seen-as-underdeveloped

"Security is … on the lower end of the development cycle for a lot of these companies"

Executive Summary

For fintech companies, protecting client data is essential, but experts say cybersecurity often takes a back seat to bringing a new product to market quickly.

Full Article

Fintech firms face related cybersecurity challenges: warding off a theft or breach and meeting regulatory standards on security. While many fintech companies know they must implement appropriate protections, that recognition is spreading slowly throughout the industry.

"People are focusing far too much on the 'tech' side and not enough on the 'fin' side—and the financial side is very heavily regulated," says Sara Hanks, chief executive and co-founder of CrowdCheck, a crowdfunding advisory firm. "The more you're shifting stuff around on the internet, the more somebody is going to intercept it, and I think security is probably on the lower end of the development cycle for a lot of these companies."

In June, a hacker stole nearly $60 million from the Decentralized Autonomous Organization, a fund for the virtual currency Ethereum. And in 2015, Venmo, a popular mobile payments company, faced a public backlash amid reports of security vulnerabilities that allowed thieves to debit money from unsuspecting users' bank accounts. [1] Small and midsized businesses of all kinds, including fintechs, remain vulnerable as various kinds of cyber incidents increase in frequency and sophistication. [2]

Mercedes Tunstall, a consumer finance attorney in Washington who also works on cybersecurity and privacy issues, notes that many fintech startups store their data in the cloud, a good first step toward protecting sensitive information. Cloud storage systems, such as those offered by Google and Amazon, already have strong cybersecurity protections.

But beyond that point, many companies find that efforts to shore up their systems against attack conflict with their central focus of bringing a product to market quickly, says Tunstall. Entrepreneurs often are keen to plow any profits back into the business rather than into cybersecurity.

Attorney Mercedes Tunstall: Efforts to shore up system security conflict with bringing a product to market quickly.

"A lot of the fintechs say, 'We know that there can be better controls and better security, but we don't have time for that, because we need to start proving our idea,' " Tunstall says. "It's a tension that's almost not resolvable between a startup trying to prove its concept and the security requirements that are really appropriate for a lot of what they're doing."

A major breach could weaken public acceptance of emerging financial technology, experts say. "In addition to causing immediate financial losses, breaches can undermine longer term confidence in new solutions, leading to lower adoption rates—particularly among users with less experience engaging with digital services," said John Villasenor, a professor of engineering and public policy at UCLA, in Forbes. [3]

Fintech firms must contend with security issues that arise not only from outside sources but also from their own users. Critics raised questions about online lender Prosper in 2015 when it arranged a loan for Syed Rizwan Farook a few weeks before he opened fire on an office holiday party in San Bernardino, Calif. There was no evidence that the lender did anything wrong or that the crime could have been detected, but the incident underscores the multitude of security challenges facing fintech firms. [4]

The regulatory landscape for fintech cybersecurity continues to evolve, as government officials consider how best to oversee these new entities.

Fintech firms have fewer regulatory requirements for cybersecurity than banks, which have some of the strongest, especially in the United States. The Federal Trade Commission (FTC) has jurisdiction over data protection, while the Federal Financial Institutions Examinations Council (FFIEC), an interagency body for the banking industry, provides technology standards for financial institutions under the supervision of bank regulators and the Consumer Financial Protection Bureau (CFPB). The FFIEC guidelines can be instructive for fintechs, even if not all of the provisions apply because the firms are not depository institutions, according to Tunstall. Many fintechs may also be subject to anti-money laundering rules, which require financial institutions and others to monitor funds in their systems for signs of illegal activity.

Regulators are still testing the waters when it comes to enforcing laws on the books against fintech companies, though several recent

examples suggest they are watching new startups closely.

The CFPB fined online payment platform Dwolla $100,000 in March because it deceived consumers about the quality of "its data security practices and the safety of its online payment system," according to a press release. It also required the company to fix its data standards. [5]

Similarly, the Financial Crimes Enforcement Network, a bureau of the Treasury Department that deals with money laundering and terrorist financing, announced a $700,000 enforcement action against Ripple Labs, a virtual currency startup, last year for failing to follow anti-money laundering rules. The company was ordered to get its compliance program in order. [6]

About the Author

Victoria Finkle is a freelance journalist based in Washington, D.C., who focuses on business, banking and public policy. She has written for the New York Times, Inc. magazine, Bloomberg BNA and Washington Monthly, and previously worked as a staff writer for the American Banker newspaper, covering Capitol Hill and consumer finance. Her previous report for SAGE Business Researcher was on behavioral economics.

Notes

[1] Alison Griswold, "Venmo Money, Venmo Problems," Slate, Feb. 25, 2015, http://tinyurl.com/q4sykof.

[2] Paul Vigna, "Fund Based on Digital Currency Ethereum to Wind Down After Alleged Hack," The Wall Street Journal, June 17, 2016, http://tinyurl.com/hudatvy; "Cyberattacks on the rise:
Are private companies doing enough to protect themselves?" PwC, http://tinyurl.com/haev3ce.

[3] John Villasenor, "Ensuring Cybersecurity In Fintech: Key Trends And Solutions," Forbes, Aug. 25, 2016, http://tinyurl.com/zw9nv7j.

[4] Noah Buhayar and Tracy Alloway, "Prosper Said to Arrange Loan to San Bernardino Shooter," Bloomberg, Dec. 8, 2015, http://tinyurl.com/zabjxop.

[5] "CFPB Takes Action Against Dwolla for Misrepresenting Data Security Practices," press release, Consumer Financial Protection Bureau, March 2, 2016, http://tinyurl.com/gkp775j.

[6] Ryan Tracy, "Treasury Penalizes Ripple Labs, in First Action Against Virtual Currency Exchange," Wall Street Journal, May 5, 2015, http://tinyurl.com/zelr2xp.