

**ÆLEX**

**CYBERCRIME AND CYBERSECURITY:  
FINTECH'S GREATEST CHALLENGES <sup>1</sup>**

AUGUST 2019

A person wearing a dark hoodie and a balaclava is shown in profile, looking intently at a laptop screen. The scene is dimly lit, with the primary light source being the laptop's display, which casts a glow on the person's face and hands. The person's hands are positioned over the keyboard, suggesting active use of the device. The background is dark and indistinct, emphasizing the subject and their interaction with the technology.



## BACKGROUND

The arrival of financial technology (“FinTech”) companies can be traced to a number of regulatory changes made after The Great Depression of the 1920s.

Among others, the United States Banking Act—which separated commercial banking from investment banking (and thus, limited the interest that a regular bank depositor could get on his deposit) –spurred, in the 1970s, the emergence of asset management firms and other forms of shadow banks—or what is now called FinTech companies.

However, it was the global financial crisis of 2008, and the near-collapse of the financial system, that caused the rise of FinTech companies and activated the FinTech transformation that the world is currently witnessing.

This article examines how cybercrime affects FinTech companies—mostly startups—and how these companies protect their data and infrastructure. It is nonetheless important to bear in mind that established financial institutions who now invest in, develop, or adopt financial technologies to improve financial services delivery and processes

(and that’s almost every bank in the world) are also captured in the article, for they too are part of the FinTech ecosystem.

As a starting point, the legal and regulatory facet of cybercrime and cybersecurity will be considered.

### **CYBERCRIME AND CYBERSECURITY: THE NIGERIAN LEGAL LANDSCAPE**

According to the Cybercrimes (Prohibition, Prevention, etc) Act 2015 (the “Act”), any person, who without authorisation or in excess of authorisation, intentionally accesses in whole or in part, a computer system or network, with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, commits an offence.[2]

The Act also makes it an offence for any person to engage in damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system.[3] Finally, the Act criminalises such other cybercrimes as: system interference, electronic theft, spamming, spreading of viruses or malware, identity theft, phishing, and denial-of-service-attacks. [4]

[1] Appreciation goes to Steve C. Morgan (Founder & CEO at Cybersecurity Ventures), for his kind permission to use the 2019 Official Annual Cybercrime Report in preparing this article. Abolore Salami, (Founder & CEO at Riby Finance) and Kofi Genfi (Director of Strategy, Mazzuma) also made important contributions to this article.

[2] Section 6 of the Cybercrimes (Prohibition, Prevention, etc) Act 2015

[3] Section 16 of the Cybercrimes (Prohibition, Prevention, etc) Act 2015

[4] See generally Part III of the Cybercrimes (Prohibition, Prevention, etc) Act 2015

One of the most important Nigerian regulations on cybersecurity is the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers ("the Guidelines"), which provide a risk-based approach to managing cybersecurity risks.

Among other things, the Guidelines mandate every company which fall under the payment service providers[5] category to: (i) adopt cryptographic controls such as public key infrastructure, hashing and encryption to guard confidential and sensitive information against unauthorised access; (ii) develop a data loss/leakage prevention strategy to discover, monitor, and protect sensitive and confidential business and customer data/information at endpoints, storage, network, and other digital stores, whether online or offline; and (iii) identify vulnerabilities in their assets by engaging professionals in this field to conduct Penetration Tests annually.[6]

There is also the new Nigeria Data Protection Regulation which, among other things, regulates how data can be harvested, stored, and processed.

## **THE GLOBAL COSTS OF CYBERCRIME AND CYBERSECURITY**

Cybercrime encompasses every illegal activity which aims to compromise the integrity of computer systems or which is designed to manipulate, illegitimately access, or compromise electronic data.

The term also refers to the deliberate use of computer networks to advance criminal causes.

Cybercrime is on the rise and does not appear to be going down anytime soon, what with the advent of such technologies as: artificial intelligence, Big Data, and cloud computing. Moreover, cybercrime is easy and largely rewarding; and with the growing number of devices connected to the internet, there is bound to be an increase in cybercriminal activities.

A low-risk, high-yield activity, cybercrime is "one of the biggest challenges that humanity will face in the next two decades." [7] According to Cybersecurity Ventures, cybercrime "will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015.

This represents the greatest transfer of economic wealth in history... and will be more profitable than the global trade of all major illegal drugs combined." [8] Alongside the rest of the world, Nigeria is also caught in the crosshairs: her economy continues to bleed from the spree of cyberattacks and breaches—last year alone, phishing attacks, ransomware, and malicious software embedded at payment interfaces cost Nigerian companies billions of Naira.[9]


[5] Payment Service Providers are third parties that allow merchants to accept a wide variety of payments through a single channel.

[6] See Generally Appendix III of the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018.

[7] Cybersecurity Ventures Official Annual Cybercrime Report, 'Cybercrime Damages \$6 Trillion By 2021' (Herjavec Group, 2019) <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/> Accessed 2 June 2019

[8] Ibid.

[9] Tope Aladenusi, 'Nigeria Cyber Security Outlook 2019' (Deloitte, 2019) <https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2019.html> Accessed 9 June 2019.



Cybersecurity refers to every coordinated measure, technique, or framework designed primarily to maintain the security of digital infrastructure, systems, and processes.

Cybersecurity involves every strategy that enables a person or entity to minimise, isolate, and eliminate cybercrime and threats. “Unfortunately, cyber adversaries have learned to launch automated and sophisticated attacks... and keeping pace with cybersecurity strategy and operations”[10] has become a particularly complex task.

Driven by increasing sophistication in technology and stricter data protection regulations, “[t]he cybersecurity market is expected to grow from USD 152.71 billion in 2018 to USD 248.26 billion by 2023, at a Compound Annual Growth Rate of 10.2% during 2018–2023,”[11] and Cybersecurity Ventures predicts that “global spending on cybersecurity products and services will exceed \$1 trillion cumulatively over the next five years, from 2017 to 2021.”[12]

These figures are huge: and some sources estimate that they may actually be higher because many entities do not accurately report their spending on cybersecurity for reputational and business reasons. This makes sense, especially since many companies see monies and resources spent on cybersecurity as ‘cost of doing business.’

In summary, cybercrime and cybersecurity are very costly matters. Together, they are interconnected phenomena that can hardly be separated: independently, they have significant financial implications for FinTech, the world’s financial system, and the global economy.

## **CYBERCRIME, CYBERSECURITY, AND FINTECH**

As FinTech companies and start-ups continue to disrupt the global financial landscape, a peculiar feature and perhaps their biggest advantage is that they are not held back or burdened by law, regulations, or existing systems.

Also, they are more agile, more aggressive, and more willing to explore and make risky choices. But this adventurous attitude and total dependence on technology to aid financial services delivery may also be their greatest weaknesses.

Only last year, an advanced, persistent team of cybercriminals hacked Taylor, a new FinTech company in Brazil and stole roughly \$1.5 million. This was shortly after another cyber heist where a whopping \$9.8 million was stolen from CypheriumChain.[13]

[10] Cyberpedia, ‘What is Cybersecurity’, (Paloalto Networks) <https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security> Accessed 12 June 2019

[11] Mr. Shelly Singh, ‘Cybersecurity Market worth \$248.26 billion by 2023’ (MarketsandMarkets, 2019) <https://www.marketsandmarkets.com/PressReleases/cyber-security.asp> Accessed 10 June 2019

[12] Steve Morgan, ‘2018 Cybersecurity Market Report’ (Cybersecurity Ventures, May 21, 2017) <https://cybersecurityventures.com/cybersecurity-market-report/> Accessed 10 June 2019

[13] Alex Hall, ‘Fintech Company Taylor Hacked, \$1.5 Million in Ether Stolen’ (eBitNews, May 27, 2018) <https://ebitnews.com/2018/05/27/fintech-company-taylor-hacked-1-5-million-in-ether-stolen/> Accessed 16 June 2019



Like FinTech start-ups, banks and other established financial institutions which adopt FinTech solutions are also at huge risk.

Recently, “criminals used stolen information from 3,000 accounts at a South African bank to make 14,000 fraudulent withdrawals from 1,700 ATMs across Japan.

The scheme took advantage of 24-hour ATMs that allow withdrawals from foreign credit cards without requiring a chip. In the span of three hours early on a Sunday morning, roughly 100 “withdrawal mules” were able to collect about \$17 million in cash.”[14]

But here is the difference between FinTech start-ups and established financial institutions: major financial institutions have been known to invest in defences to combat fraud and data theft, have better fraud prevention mechanisms, and largely comply with regulations designed to prevent cybercrimes that pose a systemic threat to financial stability.[15]

Again, banks and other financial institutions have a rich history of resilience and have, collectively, built a trusted brand. FinTech companies, on the other hand, historically fall a little short on these fronts.

Currently, FinTech companies in most countries are not bound by any serious legal and regulatory regimes, focus more on scaling and evolving, and many simply do not have the resources to build suitable security infrastructure.

Because FinTech companies do not have the resources that most banks ordinarily possess, they find themselves more exposed.

Yet, as FinTech companies and activities increase and grow, their impact and influence are increasingly woven into the fabric of the financial system—this means that the vulnerabilities associated with FinTech may well cripple the financial system, if not managed adequately. And vulnerabilities are cybercriminals’ delight.

To make things worse, it is a fact that FinTech solutions are heavily reliant on technologies (which are prone to hacking) and data (which are rich and susceptible to manipulation and abuse)—these factors combine to form the perfect recipes for disaster.

In other words, FinTech companies’ reliance on technology and use of data raise peculiar security challenges and place them in a particularly challenging situation.

[14] John Lewis, (2018) ‘Economic Impact of Cybercrime—No Slowing Down’: CSIS, pg. 21  
[15] Ibid.



The sort of highly-sensitive personal and financial users' information that these FinTech companies keep in their database and leverage on to provide personalised, predictive, and seamless financial services, makes them a very attractive target for cybercriminals.[16]

Another big problem lies in FinTech's tendencies to abandon conventional authentication mechanisms such as passwords and Personal Identification Numbers (PINs) and rely more on biometric sensors, one-time passwords, code-generating apps, etc., in a bid to deliver seamless, innovative services.

This proclivity, combined with FinTech companies' aggregation of data from diverse sources in order to provide insight-based customer experience, leaves them dangerously exposed.

And while these companies already face the mounting task of maintaining and expanding their operations and making profits, they now have to deal with the mounting cost of protecting their customers, data, and entire operation from cyberattacks.

## **HOW FINTECH COMPANIES CAN PREVENT CYBERATTACKS**

To stay protected and safe from cyberattacks, FinTech companies—and banks—must now see constant employees' education as priority. They must train their personnel and teams on

data protection and disaster management, build and maintain cybersecurity infrastructures designed to detect, withstand, and repel cyber threats, and promptly report cases of cyberattacks, as required by law.

By way of suggestion, FinTech companies should look into employing keyless encryption and “hashing techniques—which serves as an extra line of defence in case of breach—in storing all passwords and [other] sensitive data.”

In addition to this, companies that handle branded credit cards issued by card schemes should secure sensitive card data by ensuring that they are the Payment Card Industry security standard.

To further bolster safety, it is recommended that FinTech companies should conduct constant risk assessment and natively integrate automated next-generation security systems “designed to provide consistent, prevention-based protection—on the endpoint, in the data center, on the network, and in public and private clouds,”[17] and to limit the amount of data that can be gleaned from any compromise or breach. It is also recommended that FinTech companies should take steps to reduce incidences of eavesdropping and man-in-the-middle attacks by segregating mission-centric data from routine information, and by incorporating layers of protection and layers of access to critical information. [18]

[16] For example, according to Interswitch's privacy policy, the company routinely collects personal data such as name, address, phone number, and email addresses and financial information such as full bank account numbers and/or credit card numbers. (See <https://www.interswitchgroup.com/ng/privacy-policy>) Accessed 10 June 2019

[17] Ibid (n 6)

[18] Adapted from a 2012 Remark delivered by Robert S. Mueller, III, Former Director, The Federal Bureau of Investigation, (March 1, 2012) <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies> Accessed 11 June 2019



From a legal standpoint, we recommend that FinTech companies ensure total compliance with the Data Protection Regulation and related laws—pursuant to this, every company should collect the minimum required data, implement information security standard, and designate a full-time data protection compliance officer to guide their processes and shield their operations from regulatory fines.

Further, we recommend that FinTech companies disclose in their privacy policies the sort of personal and financial information they collect, how this information is stored, processed, or shared, and steps taken to protect this sensitive information from theft, compromise, or breach.

FinTech companies should have in place policies and procedures for monitoring and reporting violations of privacy and data protection, and—where a FinTech company finds its systems or data compromised through cyberattack—steps should be promptly taken towards reporting breaches. Failure to do so may attract serious sanctions.

## CONCLUSION

From payments and remittances to lending and wealth management, FinTech continues to change the way we live and bank. But by virtue of their operations, FinTech companies constitute a particularly attractive target for cybercriminals and have to take the

complex challenge of cybersecurity seriously. They must invest as much in cybersecurity as they expend on expanding their reaches and scaling their operations.

Also, they must build a solid plan and acquire the resources to fight relentless, unseen, and largely unknown enemies—for operating in a connected world bears grave consequences.

“The future of Fintech is promising, and it would be a shame to see its activities cut short by pitfalls that could have been avoided”[19]—the biggest of which is cybercrime.

Players in the FinTech space must always remember, therefore, that no one is immune from cyberattacks, and no one is completely safe. As Robert Mueller once said: “There are only two types of companies: those that are already hacked and those that will be.”[20]

To survive in an increasingly vulnerable digital world, FinTech companies may have to always bear this nightmarish truth in mind in carrying out their daily transactions.

[19] Signaturit, ‘What legal and security risks does Fintech face?’ (January 19, 2016) <https://blog.signaturit.com/en/legal-and-security-risks-for-fintech-startups> Accessed 10 June 2019.

[20] Ibid. (n 14)

# ÆLEX



Ademola  
Adeyoju

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed [here](#). You can also visit our website at [www.aelex.com](http://www.aelex.com) to learn more about our firm and its services.'

**COPYRIGHT:** All rights reserved. No part of the publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior permission in writing of ÆLEX or as expressly permitted by law.

**DISCLAIMER:** This publication is not intended to provide legal advice but to provide information on the matter covered in the publication. No reader should act on the matters covered in this publication without first seeking specific legal advice.

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana.

Contact us at:

4th Floor, Marble House,  
1 Kingsway Road, Falomo Ikoyi,  
Lagos, Nigeria

Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,

E-mail: [lagos@aelex.com](mailto:lagos@aelex.com)

Click here [www.aelex.com](http://www.aelex.com)

to follow our social media handles  
click below

