Security at Stash
Whitepaper: Guide to Payment Data Security for Fintech Companies

For fintech startups and companies that process payments, nothing is more sacred and valuable than private cardholder data. But protecting that data from hackers, cyber attackers, and malicious actors is getting harder than ever. In fact, nearly three-quarters of all hackers say that they’re constantly testing new systems and technologies, and are convinced they can compromise any target in less than 12 hours.

Fintech companies that process payments or handle sensitive financial customer data can - and should - take steps to secure critical systems and information. It’s also important to understand both the threat and regulatory landscapes that affect fintech companies so that any cybersecurity strategies and tactics address major security gaps and do so in a compliant fashion. You’ll also want to select the right technology and cybersecurity partners to help you evolve and adjust to emerging threats over the long run.

In this whitepaper, you’ll learn:
• The biggest cybersecurity threats all fintech companies should be aware of
• Key regulatory frameworks that fintech companies need to comply with
• Fintech cybersecurity best practices from industry experts
• Selecting the right technology and cybersecurity partner

Digital payment transactions are increasing year-over-year. Source: Statista - https://www.statista.com/outlook/296/100/digital-payments/worldwide#market-revenue
1. Fintech Security Threats

Before you can begin strategizing about how to best protect sensitive and confidential payment data that your fintech company handles, you need to first be aware of the specific threats you’ll likely face. This includes both imminent threats and those fintech companies are likely to face in the not-too-distant future. Here are some of the biggest ones you need to be aware of:

**Phishing**

One of the oldest methods of gaining unauthorized access to financial data, phishing still remains one of the biggest threats to fintech companies and the digital banking ecosystem in general. Phishing attacks continue to grow in sophistication and can now even be done through **SMS banking transactions**. Phishing hackers seek to obtain a user’s login credentials - via fake emails or text messages - and gain access to their private banking data. Cybercriminals can even use a customer’s login as a “back door” to other, more mission-critical aspects of your payment systems.

Phishing used to be easy to identify. Poor spelling and grammar were dead giveaways, as was the non-personal nature of the email. Well, the “Dear sir/madam” intro has been replaced by very targeted messaging. “CEO Wire Fraud” attacks accounted for $2.3 billion in losses, according to the FBI. This “spear-phishing” features language that is very specific to the recipient, and often high-level folks with top access and the ability to authorize payments.

**Malware**

One of the biggest threats to digital payments - and the financial sector at large - as evidenced by the recent hack of cloud accounting software provider Wolters Kluwer. The $4.8 billion company was forced to shut its system down for prolonged periods to prevent malware from spreading, while thankfully no sensitive client financial data was shown to be accessed. Fintech companies represent prime targets for malware attackers, especially when it comes to cardholder data used in payments.

Fintech companies need to take extra precautions against malware since 25 percent of all malware is targeted towards financial institutions. Banking Trojans are some of the earliest
threats that hackers use to target financial institutions and clean out bank accounts en masse. Implementing and having robust firewall and antivirus software running regularly on all devices will help you handle sensitive customer data in a more secure fashion.

**IoT Attacks**
The Internet of Things (IoT) is rapidly taking hold in both business and household. And devices like Amazon Go and Siri are increasingly used in payment transactions. And with most IoT devices being internet-enabled, the IoT ecosystem is certainly at risk of being hacked. The 50 trillion gigs of data that IoT devices will have sent out by 2020 is at risk of being accessed by the most sophisticated of hackers. This makes changing your fintech company’s passwords and factory security settings when employing these devices paramount to long-term privacy success.

The FBI said in a recent notice, that cybercriminals usually compromise IoT devices by taking advantage of weak authentication or obsolete firmware, or via brute force attacks on devices with default usernames and passwords. These bad actors use these compromised devices as proxies for their Internet requests to route malicious traffic for cyber-attacks and computer network exploitation.

**Cloud Hacking**
Storing, processing, and backing up data on a cloud server has become standard protocol for most organizations. This enables immediate control, accessibility, and collaboration opportunities, but it also puts data at risk. This is one of the reasons why cloud hacking is taking root as a common mode of attack for hackers, leaving some fintech companies wary of deploying sensitive customer data in the cloud..

To avoid cloud hacking threats, stay away from using the public cloud for your fintech company as this will only increase your chances of a data leak. To achieve the best results, fintech firms would be better off acquiring their own private cloud server for data storage due to their superior security prowess.

**STASH**
This goes to show that even in this hyper-secure world that we live in, security breaches are still commonplace. The growing dependency of numerous organizations on big data means that personal and proprietary data is possibly compromising and can be breached and accessed by malicious entities. This is why having solid controls in place is helpful to ensure you’re able to at least implement a skeleton structure that makes sense for your business.

2. The Regulatory Landscape

The fintech landscape is constantly evolving due to regulators experimenting with tools that might improve oversight of the industry. These frameworks are put in place to ensure customers are fully protected in a way that doesn’t stifle innovation.

Regulators are also constantly seeking to gain new perspectives on fintech that can help them design adequate protection policies that are friendly to innovators. This makes it important for fintech innovators to become more attuned to key concerns and issues, especially regarding consumer data protection and cybersecurity.

Keep a Close Eye on Blockchain Regulations

Of all the emerging innovations in the fintech industry, blockchain technology is arguably the
one that’s generating the most buzz. This decentralized and open digital ledger creates a real-time chain of encrypted blocks of all past transactions. This allows blockchain to provide faster, more transparent, and effective functions that can pave the way for less costly financial transactions in the future.

As the adoption of blockchain by fintech startups has increased, regulators have caught on to how cost-effective this transparent ledger is from a regulatory perspective. Blockchain also can improve information security and help to better predict, identify, and analyze fraud which earns fintech companies points with regulatory authorities.

Although blockchain is incredibly useful for its speed, transparency, and security, it is not without certain weaknesses. The blockchain operates on a decentralized system, meaning a breakdown in one area of the system could spread like wildfire in a matter of seconds to other financial markets.

**PCI DSS Compliance for Fintechs**

Many fintechs like Stash pursue compliance with the Payment Card Industry Data Security Standard, or PCI DSS for short. PCI security standards are both technical and operational requirements set forth by the Payment Card Industry Security Standards Council to protect cardholder data. PCI DSS govern all merchants and organizations globally that store, process or transmit this data.

The types of data that PCI DSS is designed primarily to protect the cardholder’s card number, name, and any other personal information associated with that account. Moreover, compliance with PCI DSS also requires companies to protect other sensitive data associated with the card, such as PIN codes and other secondary information that might be used to verify the account. PCI DSS even sets security standards for the magnetic strip of any given card.

But what’s important to fintech companies is that PCI DSS standards also include specific requirements for software and app developers whose products are used in debit or credit card transactions. Moreover, PCI DSS compliance is becoming increasingly important for smartcard transactions. Take Stash’s Stock-Back debit card, for example, that rewards debit card users in
the form of stock equity investments. For transactions taking place on the Stock-Back card, Stash has taken PCI DSS compliant measures to protect cardholder data in areas like firewall security, system access controls, and regular network penetration testing.

PCI DSS also spells out various levels of compliance that any fintech or payment software developer has to reach. This depends on the number of cardholder records the system holds at any given time, as well as the amount of transactions processed on a regular basis. In general, most fintech companies will need to conduct an annual penetration tests and PCI scan by an approved scanning vendor (ASV), accompanied by an Attestation of Compliance (AOC) certificate that demonstrates to customers and regulatory bodies that your software is PCI DSS compliant.

**GDPR and Fintech Regulations**

Until recently, financial results have traditionally been presented annually and quarterly to regulatory authorities. Now, GDPR mandates reporting of data breaches within 72 hours which shows how important it is to embody the idea that fast online transactions must demand equally fast regulatory capacities. Over time, even this timescale will appear obsolete as more focus is put on real-time transaction monitoring.

Although the world has yet to reach a global standard for a financial regulatory framework, GDPR is helping to enlighten governments about the threats to payment data security. As of now, the dual system of federal and state regulation in the U.S. poses substantial challenges for fintech companies to identify the applicable legal and regulatory frameworks. This domestic regulatory framework will most likely change over time thanks to the influence of GDPR, which will surely have a lasting effect on financial industries for the foreseeable future.

**3. Cybersecurity Best Practices**

“The first recommendation I have is that if you don’t need the data, don’t store it. Better yet, don’t even collect it in the first place,”

*Gavin Grisamore, VP - Head of Information Security @ Stash*
One of the biggest payment data security mistakes that fintechs make is collecting and storing data necessarily. This can put you in scope for other compliance issues as well as other regulations such as GDPR if you’re an international company. If you operate in California, for instance, you’re also likely subject to the California Consumer Privacy Act (CCPA).

Banking customers, for example, might need to provide information in order to link another bank account to their existing ones. What the fintech solution should do after collecting the user’s bank routing number, account number, username, and password is to then hand it over to a third-party that’s already integrated into the existing technology stack. This pushes all of the risks to the third party tool to be able to manage those credentials, thereby reducing risk your organization’s risk.

Also make sure not to collect sensitive information internally because it could show up in a log file if you’re not careful. If you’re needlessly collecting a plethora of information, it’s then your responsibility to store that information, secure it, and provide it every type of protection that it needs. Depending on what type of data you’re working with will put you in a different scope for compliance or regulatory issues.

Next, when you’re storing any data, make sure to use encryption best practices. Regardless of what datastore the information is in, it should be encrypted at rest. When you’re moving that type of data from one datastore to another, all of those channels should be encrypted as well.

Lastly, we start to get into access control which determines who can access what type of data you have. Make sure that your customer support team is able to see certain information about your customer accounts to help troubleshoot login and account-related issues. Make sure that these actions are audited, that there are limitations to how much access they have, and that there is an escalation path for harder to troubleshoot items that a senior manager or someone else might need to handle.

4. Technology Strategies & Partners

Innovative technologies and processes have both played their own crucial role in helping fintech startups to scale effectively as a supplement to their cybersecurity partner solutions.
Here are a couple of strategies that fintech companies can use to become more adept at keeping a strong data security profile:

**You Have Permission to Scale**
When your fintech startup is in its infancy stages, you may not want your network permissions to ever expire because not many permissions exist and your team is small enough to handle them all. Once your startup begins to grow and you begin adding more employees and permissions, you definitely want your permissions to expire at some point. However, it can be cumbersome to rotate them every quarter like clockwork.

This is why growing fintech companies must select a cybersecurity partner that can verify when an employee logs into the system every day. From there, the system will issue the employee their unique, temporary credentials that they need to access the portion of the database that they need to do their job. This helps to reduce fintech risks tremendously because if a hacker were to gain access to a key, it could only be used for one day.

**Access Control is King**
In fintech organizations, it’s common to give developers the ability to take a snapshot or a backup of the database and copy it into a new database for instances of disaster recovery. This process of giving developers the ability to create database snapshots can either be used as a means for collecting information or as an avenue for them to steal the information. If you provide an extra level of authenticity such as two-factor authentication (2FA) to be able to approve that action, you can deter the possibility of the information being stolen.

Things get bad for access control either from an insider threat standpoint or when an employee gets caught in a phishing scam and their computer is compromised (if, in fact, their credentials were stolen when their computer was compromised). Once a computer is compromised, the hacker will pretend to be that user to obtain further network access. This is why tightening up your access controls can help your fintech company mitigate the possibility of having a data breach of epic proportions.
Key Takeaways

Overall, fintech is a great ecosystem that has managed to disrupt the antiquated financial industry. It has also made people realize that money exchange, investments, insurance, and other financial services are going to radically change in the next decade and make our lives better. But, no matter how much fintech is projected to change the world, we cannot forget how the evolving threat of cyber-attacks will continue to make the prospect of increased payment data security difficult to sustainably deploy.

Fintech companies must understand how to minimize the impact of the types of cyber threats that were addressed in this whitepaper and think constantly about progress to alleviate any negative effects that a data breach entails. Keeping abreast of the key regulatory frameworks that your fintech company must comply with, following key cybersecurity best practices will help you scale. In the end, it is in the selection of the right technology and cybersecurity partner that will help you grow exponentially.

Resources

- [https://gomedici.com/7-security-mistakes-fintech-easily-avoid/](https://gomedici.com/7-security-mistakes-fintech-easily-avoid/)
- [https://www.spreadly.com/blog/hacking-payment-forms](https://www.spreadly.com/blog/hacking-payment-forms)