Published on *The National Law Review* https://natlawreview.com

FinTech Companies Face Big Privacy Challenges in 2016

Article By:

Natalie A. Prescott

Cynthia J. Larose

According to the FBI, "there are only two types of companies: those that have been hacked and those that will be." It does not take an actual data breach, however, for a company to be liable for its data security practices. In March 2016, the ***Consumer Financial Protection Bureau (CFPB)*** made this clear when it settled its first-ever data security enforcement action against an online payment processing company, Dwolla. The CFPB pursued Dwolla because it found the company's representations to customers about its cybersecurity misleading – disregarding the fact that Dwolla had never, since its inception, experienced even a single reported cybersecurity incident. As a part of the settlement, Dwolla agreed to sign a Consent Order, pay a $100,000 fine, take certain steps to improve its data security for the next five years, and make accurate representations to consumers. The *Dwolla* case offers important guidance to FinTech companies and provides a framework for data protection and preparedness plans.

The Story of Dwolla Illustrates Startup Privacy Pitfalls

A young FinTech company, Dwolla first launched in Iowa with just two employees. Small but persistent, it secured funding and eventually grew to over 650,000 consumers and $5 million in daily payment transfers. Even the U.S. Treasury Department's Bureau of Fiscal Service saw its potential and included Dwolla – alongside with the industry giant, PayPal – in its online payment system in 2015.

But that was not how Dwolla became famous. As the company learned the hard way, today's consumer privacy protection is different from what it was years ago. Where previously FinTech companies caught consumers' attention through fast growth and innovations, they are now capturing the government's attention with their outdated cybersecurity practices. This was the case for Dwolla.

Dwolla's Case Offers a Cautionary and Valuable Lesson

The CFPB investigated and sued Dwolla for its public representations to customers that its transactions were "safe" and "secure," that its information was "securely encrypted," and that it was compliant with up-to-date data security standards. The CFPB is not the first federal or state agency to warn companies that privacy policies must "say what they mean, and mean what they say."

The *Dwolla* case highlights the need to be proactive and to implement proper security protocols, which can avoid the breach altogether or at least negate the risk of penalties. What it leaves unresolved, however, is (1) to which extent FinTech companies may benefit from proactively reporting cybersecurity breaches and concerns, (2) whether various regulators intend to collaborate by a way of uniform guidelines and joint enforcement actions, and (3) if the companies may seek advisory opinions from the CFPB on their current practices.

The CFPB Joins Other Regulators in the Privacy Enforcement Arena

While *Dwolla* was the first-ever privacy and security action by the CFPB, other regulators have long ago entered the field. They include the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), Commodities Futures Trading Commission (CFTC), the National Futures Association (NFA), the Department of Justice (DOJ), the Federal Trade Commission (FTC), and state Attorneys General.

The *Dwolla* action is most noteworthy, however, because the CFPB did not wait until an actual data breach. In an aggressive move, the CFPB prosecuted Dwolla despite lack of harm. The CFPB used *Dwolla* as a test case, (1) to provide guidelines to other companies on what it believes to be reasonable and appropriate in the arena of privacy protection, and (2) to warn other FinTech companies whose privacy practices may be non-compliant. This action should provide a warning to younger startups, which may not have fully vetted cybersecurity policies in place – if privacy policies have been reviewed at all. And it is a clear sign that the agencies are becoming more proactive with respect to data-privacy regulatory actions.

The CPFB is following the Federal Trade Commission's path in bringing this enforcement action. Its authority under 12 U.S.C. § 5531(a) allows it to regulate "unfair," "deceptive," and "abusive" practices, akin to the powers granted to the FTC under the FTC Act. Under what is known as the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPB can take actions against financial companies that misrepresent privacy safeguards. Importantly, the CFPB can also seek fines for non-compliance. The Act further requires all companies that offer financial services to abide by the consumer-financial-protection regulations.

The *Dwolla-Wyndham-HTC* Decisions Finally Establish Clearer Privacy Guidelines for U.S. Companies

Although most legal commentators focus exclusively on *Dwolla* and the CFPB, the *Dwolla* consent order has a much broader implication. This action was not just about the CFPB or an isolated incident of misstatements about online security. When read together with other key enforcement actions, the *Dwolla-Wyndham-HTC* trifecta represents the clearest guidelines the financial industry has available to date. In many respects, the *Dwolla* consent order builds on the foundation set forth by the *Wyndham* and *HTC* enforcement actions discussed below and then further expands on it by imposing penalties. And, although the CFPB has not previously issued clear guidance in this arena, the *Dwolla* case now fills that gap.

By way of background, Wyndham Hotels and Resorts experienced three major data breaches in 2008-2009 that compromised consumer information and led to over $10 million in unauthorized credit card charges. The FTC brought an action against Wyndham in federal court, which settled last year. The gist of the lawsuit was the allegation that Wyndham engaged in "unfair and deceptive practices" because it promised customers to follow rigorous security standards while its actual standards were

inadequate. The company argued that there were no clear guidelines and no fair notice from the FTC. The court disagreed, noting that the FTC's guidance documents, enforcement actions, and prior settlements provided sufficient notice as to what measures are reasonable. In the end, the FTC required the company (1) to "establish a comprehensive information security program designed to protect cardholder data," (2) to conduct annual information security audits, and (3) to "maintain safeguards in connections to its franchisees' servers." Yet, despite evidence of actual consumer harm, there were no monetary penalties.

Another notable consent order originated in 2013 between the FTC and HTC America Inc. There, again, the FTC claimed that the company engaged in unfair and deceptive business practices, including lack of proper training and data security protocols. The FTC alleged that the company's platform had a number of security deficiencies, while representing to customers that higher-than-actual security standards were in place. In the end, the company stipulated to a 20-year-long consent decree, which required it to address current vulnerabilities and to implement a comprehensive security program.

Read together with *Dwolla*, these decisions provide an unequivocal answer to what the FTC and the CFPB expect from companies that handle consumer data.

To Prevent Data Breaches and Show Good Faith, Companies Must Follow 10 Steps

Dwolla and its progeny established a broader regulatory landscape for financial privacy and provide a practical guide to FinTech companies with respect to privacy practices. Post-*Dwolla*, companies that handle sensitive consumer information must follow these 10 steps to shield themselves from enforcement actions:

1. **Make accurate representations to customers**. Companies must review their online and direct representations to consumers and verify that their listed privacy policies and statements regarding data security are current and accurate.
2. **Regularly update privacy and data security policies**. Companies must review and routinely update their policies, ensure that they follow the latest protocols, and provide the most advance protection of consumer data. This includes a policy not to collect data unnecessarily – after all, the more data the company has, the more data it will lose in the event of a breach. Updating policies is not enough, however. Companies must also ensure that the employees actually know about and follow these policies.
3. **Prepare a comprehensive Data Security Plan**. The Plan must include safeguards for preventing a breach, steps necessary to identify a breach, and protocols to follow in the instance of a breach. Additionally, the companies should obtain cybersecurity insurance coverage.
4. **Conduct annual information security audits**. Depending on the size, FinTech companies should either conduct a smaller-scale internal audit or retain an outside auditor. The audit can identify potential weaknesses, analyze whether the current practices are up-to-date, and even uncover a breach that may have occurred and gone unnoticed.
5. **Train employees on data security**. Every employee who handles sensitive data, every manager, and all IT personnel must undergo regular mandatory training. They should know how to handle consumer data, how to spot potential breaches, how to avoid them, and where to report them.
6. **Rely on latest technology**. Companies should utilize data loss protection software, which can detect internal unauthorized data downloads. Additionally, digital rights management

software can track where sensitive data is going.

7. **Have an anti-USB policy**. Because many breaches occur from within, companies must ban the use of thumb drives, storage drives, and other removable media by employees. They should also prohibit the storage of personal consumer data on employee laptops.
8. **Always encrypt sensitive data**. Companies should password-protect sensitive documents. Employees should not send or receive identifying personal information via email. Encryption must be used for data in transit. Additionally, companies should consider double encryption, which may soon be the new golden standard for the FinTech industry.
9. **Test your operations and vet your vendors**. The IT department should be responsible for periodic testing of the operations and compliance. This includes phishing-assessment campaigns, internal audits, and analysis of individual employees' practices. Where gaps exist, additional mandatory training is necessary. Furthermore, companies must appropriately vet their vendors – who access customer data – and ensure that the vendors' security practices also meet current standards.
10. **Designate a privacy reporting manager**. Every company should have an employee responsible for privacy compliance and reporting. Employees must know where to turn in the event of a breach or lack of compliance. In larger companies, this role belongs to a Chief Privacy Officer, while in smaller firms, it may fall on the IT or HR manager. Irrespective of the title, privacy officers must have proper training and qualifications.

FinTech Startups Will Continue to Face Big Security Challenges

Cybersecurity compliance is important because data breaches are on the rise in the financial sector. This trend is noted in the Verizon 2016 Data Breach Investigations Report, A comprehensive analysis of cybersecurity threats and breaches. Last year, the Report analyzed over 100,000 security incidents and 2,260 confirmed data breaches across 82 countries. In 2015m, the Report notes, the finance sector encountered 1,368 incidents of compromised online security and 795 instances of actual data loss.

The financial industry is at the top for targeted attacks through web applications. It's "where the money is." For financial services, web app attacks are the main vulnerability and account for nearly half of all security breaches. Typically, the attack exploits code-level vulnerabilities and thwarts authentication mechanisms. Hackers are driven to financial companies for monetary gain, espionage, and information gathering to aid in a different attack. Importantly, it does not take long to infiltrate online security: In 98% of cases, financial factor systems are compromised in a matter of minutes.

Although No Uniform Privacy Laws Yet Exist, the Pressure on FinTechs to Comply is Rising

When a FinTech company becomes a victim of a cybercrime, it faces serious consequences. Data itself is compromised, the system is affected, revenues suffer, and reputational damage follows. Needless to say, for young FinTech companies and established financial institutions alike, reputation is paramount, and the consequences of a data breach can be long-lasting. The risk of consumer class actions and regulatory enforcement actions only complicates things further.

Unfortunately, U.S. Privacy and cybersecurity laws and regulations are anything but clear. They are numerous, they co-exist at the state and federal level, and there is no comprehensive and uniform regulatory system in place. There is also not one official authority in charge. As discussed above,

many different agencies seek to regulate privacy laws. But because of the sensitive nature of the information involved, FinTech companies face more pressure when compared to other industries.

FinTech Companies Face Greater Scrutiny Because They Are Intimately Involved in Consumers' Lives

FinTechs face tougher penalties for data breach, in part, because they typically collect and retain the most personal data about a large group of consumers. They are the ones most likely to have custody of particularly sensitive data. For example, companies offering mobile payment solutions may gather names, addresses, dates of birth, telephone numbers, Social Security numbers, bank account and routing numbers, passwords, and PINs.

Consumers and agencies justifiably expect the highest level of protection from the FinTech industry because of the special relationship of trust. As a result, financial companies face more scrutiny in general. In May 2016, the CFPB issued a proposed rule that would restore the customers' rights to sue financial institutions and will no longer allow them to include mandatory arbitration clauses in fine-print contracts. And The New York Department of Financial Services recently announced that it was soliciting input from other regulators on how banks and startups can bolster cybersecurity.

In short, the CFPB and other regulators believe that FinTech's access to sensitive data represents a unique threat to consumers. In a press release, the CFPB's Director Richard Cordray explained, "Consumers entrust digital payment companies with significant amounts of sensitive personal information. . . . With data breaches becoming commonplace and more consumers using these online payment systems, the risk to consumers is growing. It is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices." Lack of notice or certainty in the privacy regulatory arena will not shield the industry from the CFPB, especially since *Dwolla* and other recent enforcement actions now provide in-depth guidance.

The CFPB's Authority to Impose Fines Provides It with Greater Leverage

FinTech companies who closely followed *Dwolla* should not assume that the same lower penalties will be the standard for future actions. The CFPB's fines greatly range in size. This is why the CFPB's actions have more bite to them: In contrast to the FTC, which lacks the authority to impose fines for unfair and deceptive practices in these circumstances, the CFPB can seek monetary penalties and mandate compliance. The CFPB's Civil Penalty Fund is a depository for these collections. Since establishing the fund six years ago, the CFPB has already obtained well over $200 million in fines. This does not include more recent actions and the relatively small – in comparison – sum of $100,000 it received from Dwolla.

The CFPB uses the money to reimburse the victims (including victims of unrelated breaches) and to educate consumers on data privacy and financial literacy. In 2013, a staggering $13.8 million of these funds went towards consumer education. In short, the CFPB's ability to levy monetary sanctions undoubtedly gives it a lot of leverage in cases where there are no actual damages.

As for Dwolla, it has recently issued a public statement: "It has never been the company's intent to mislead anyone on critical issues like data security. For any confusion we may have caused, we sincerely apologize." Reportedly, "Dwolla's current data security practices [now] meet industry standards."

National Law Review, Volume VI, Number 202