# Highlights: Data Security Considerations for FinTech Companies

OCTOBER 24, 2013

In keeping with the focus of our cybersecurity and data privacy theme this week, we thought we should share highlights from an article published earlier this year by Associate Ian Wildgoose Brown in the *Bloomberg Law Banking Report*.

Five Key Legal Requirements and Five Best Practices for Complying With Them

Data security and privacy standards for companies in the financial sector are generally well-settled, at least in theory. Companies typically must maintain *reasonable* procedures to protect sensitive information. In general, applicable law requires a process-based approach to the development and maintenance of a comprehensive security program.

This means that the steps you take as a business to preempt privacy and data security breaches (as well as thoroughly documenting those steps) are of paramount importance in establishing your legal compliance. However, this determination is highly context-specific: whether your security practices are reasonable depends on the nature and size of your business, the types of information you collect or have access to, the data security tools available to you based on your company's resources, and the particular security risks your business is likely to face.

*Five Key Legal Requirements*

There is no single comprehensive body of law on liability for data security breaches. Instead there is a patchwork of federal, state, and regulatory laws whose effects vary depending on context. But the following are certain key requirements imposed by various laws that you should be aware of as a player in the finance sector.

1. **Control access to data.** Your company must have reasonable written policies and procedures to ensure the security and confidentiality of customer information and to protect against unauthorized access to or use of that information, both by third parties and your own employees. Unfortunately there are no hard-and-fast rules, and the determination of reasonableness is context-specific.
2. **Retain data appropriately.** Government agencies do not only assess whether companies have established and are complying with appropriate policies, procedures, and processes

that allow identification and reporting of suspicious activity. They also require assurance that companies can provide sufficient detail in reports to law enforcement agencies so that those reports are useful in investigating any suspicious transactions that are reported. Audits typically center on an examination of your records and require you to explain any gaps.

3. **Dispose of data properly.** The flip-side of effective data retention is appropriate data disposal. Keeping information you do not reasonably need to retain increases the likelihood of incurring liability in the event of a data security breach.
4. **Treat customers and consumers consistently with promises.** The Federal Trade Commission enforces rules requiring businesses to handle consumer information in a way that is consistent with their promises to their customers (for example, in an online privacy policy), in addition to its rules discouraging data security practices that create an unreasonable risk of harm to consumer data.
5. **Disclose breaches.** You have a general duty to disclose security breaches to those who may be adversely affected by any such breach. The kind of event that triggers a disclosure obligation varies depending on the rules specifically applicable to your business. This uncertainty reinforces the importance of having robust processes for detecting breaches that could obligate you to inform or warn your customers, the government, or others.

The objective of these standards is generally to shield your company's systems and information against unauthorized access, use, disclosure, or transfer, but also against modification or alteration, processing, or accidental loss or destruction. In designing safeguards, you should remember that the source of threats to your data security can be internal as well as external to your organization. You should also be mindful of where your customers and consumers are located: there are further legal requirements that apply if your business touches the EU. ( Directive 95/46/EC can be found here.)

*Five Practical Steps Toward Compliance*

It is important for your business to establish clear processes that effectively address data security issues. The cost of implementing security measures—particularly relative to the size of your business—is a factor in determining the reasonableness of your precautions. However, no FinTech business is exempt from the standard and any breach will be evaluated in hindsight. Your focus should be on risk assessment, and on adopting security controls that are responsive to the particular threats your company faces.

The obligations that apply to financial institutions in particular are supplemented by a set of practices, many of which are recommended by government or industry bodies, that can create "good facts" for your business as you try to establish that your data security practices are *reasonable*. The following is a general overview of some of these best practices.

1. **Have an executive officer with dedicated data security responsibility.** Your board of directors should provide strategic oversight regarding information security policy and practices. As a management team, a key procedural step is regularly reporting to the board on the adequacy and effectiveness of your company's program. You should ensure that the

board understands how critical information and information security is to your organization. A devoted data security officer with direct access to his or her fellow management team and to the board facilitates this important dialogue.

2. **Implement preconceived processes and procedures.** Reduce in-the-moment thinking, increase automation and response. Setting up internal data security controls improves your company's regulatory compliance and allows financial institutions you work with to assure themselves that they are satisfying their own regulatory compliance obligations.
3. **Implement—and use—network security protections.** Allowing confidential data to be stored outside your firewall creates opportunities for targeted eavesdropping (use of programs to analyze the way multiple programs running simultaneously on the same operating system share memory space) or relay or man-in-the-middle attacks (real-time insertion between the reader/recipient of a message and the victim of the attack). Imaginative, proactive strategies for incentivizing employees to follow seemingly-burdensome data security procedures can help address such potential risks.
4. **Be cautious about the cloud.** Public cloud services are becoming a favorite target of data thieves. And such third-party servers may be compelled to give up data in response to a subpoena—potentially circumventing privacy laws and thereby undermining customer confidence in your FinTech company in a way that is unrelated to your business and out of your control.
5. **Monitor developments and learn from past events.** A legal standard based on reasonableness is a moving target. As data security practices change, and as technology and security threats evolve in tandem, the measures you will have to take will likewise evolve. Avoid succumbing to a false sense of security by conducting periodic internal reviews and monitoring external developments and current events. Then take easily-documented and established steps in response to these reviews, implementing elements that are reasonably applicable to your business and reasonable in cost.

*Conclusion*

The financial sector's context-specific regulatory approach is likely to be put to the test as the balance of market power between established financial institutions on the one hand and startups and non-traditional industry players on the other. Traditional financial institutions may now have the advantage in emerging markets like mobile payments because they have proven security measures and solid reputations, but that could change quickly as new entrants challenge established players with new innovative offerings from equally powerful companies and nimble software-as-a-service businesses alike. A strong data security record is a valuable asset in an increasingly crowded marketplace.

Read the full article — Data Security Considerations for FinTech Companies