# *Client Alert*: FTC Reaches Settlement with Paypal over Gramm-Leach-Bliley Act and FTC Act Violations

**Related Attorneys**

Marcel C. Duhamel

**Related Services**

Data Strategy, Privacy and Security

**Related Industries**

Financial Institutions

**CLIENT ALERT** | 3.7.2018

The Federal Trade Commission (FTC) has announced a settlement with PayPal, Inc., operating as Venmo, over alleged violations of the Federal Trade Act and the Gramm-Leach-Bliley Act (GLBA). The FTC's allegations center around Venmo's disclosures to consumers about funds availability, its privacy practices and its data security practices. The settlement should serve as a warning to all financial institutions to be careful in the development and administration of "apps" and online consumer services, and to be careful about the business practices of acquired companies.

## Venmo and PayPal

Venmo, acquired by PayPal in 2013, offers "peer-to-peer" payment services to consumers via an app available on mobile devices and on the web. The FTC alleges that consumers can link external credit card and bank accounts to a Venmo account, can receive into their Venmo accounts funds from other consumers or from linked external accounts, and can transfer funds from their Venmo accounts to linked external accounts. Venmo is marketed as a method for consumers to make payments to, and to receive payments from, "anyone."

## The Alleged Conduct

Venmo's alleged practices in three areas caused it to run afoul of the FTC. First, Venmo made representations to consumers, both on the app and in its advertising, that consumers could transfer funds out of their Venmo account to a linked external account "in as little as one day" or "overnight." According to the FTC, these representations were false. Venmo in fact waited until a consumer initiated a transfer request to begin the clearing process and often either delayed the transfer for several days or outright blocked it or reversed the deposit transaction. The FTC asserts that Venmo had actual knowledge that consumers did not understand its practices yet continued them without any additional disclosures.

The FTC also focuses on Venmo's privacy practices. By default, consumers' activities are, according to the FTC, posted to the app's social networking feed and made publicly available to anyone on the internet. Users are able to change these settings, but doing so requires a confusing and multistep process that, if done incorrectly, can be overridden by the other party to a transaction. For example, a consumer could believe that she had changed her settings so that receipt of a payment would be visible only to her, but if the payor chose to make the payment public, the payment would be shown on the feed despite the payee's privacy election. This can happen retroactively, so that a consumer can elect the most private option for all transactions only to have that election retroactively overridden by a third party. Preventing this requires a consumer to follow several steps, but this is not clearly explained. Indeed, according to the FTC, Venmo's FAQs provide incorrect information to consumers about how to ensure the privacy of a transaction. Venmo also failed to send initial "clear and conspicuous" privacy notices to consumers, in that the notices:

- Were accessible via links which were printed in dark grey typeface against a light grey background;
- Were inaccurate, because the default settings made all information public while the privacy notice implied the contrary; and
- Were not delivered reasonably, because a consumer could create an account without acknowledging receipt of the notice.

Finally, the FTC takes issue with the security measures Venmo takes regarding consumer information and with what Venmo tells consumers about those measures. Venmo represents on its app and website that it employs "bank-grade security systems and data encryption" to protect financial information. The FTC alleges that, until March 2015, this representation was false. Specifically, Venmo failed to provide security notices about account changes (such as password changes or a new email address being assigned to the account). According to the FTC, these failures permitted hackers actually to take over the accounts of some consumers. Venmo also allegedly failed to have a written information security program, failed to assess reasonably foreseeable risks, and failed to provide adequate customer support to investigate consumer reports of the compromise of their accounts.

The FTC maintains that the failure to provide accurate information about funds availability, and the misrepresentations about privacy and security, violated Section 5 of the Federal Trade Act, which prohibits "unfair or deceptive" trade practices. The FTC also asserts that the privacy practices it alleges violate the GLBA and its Privacy Rule, and that the security failures it alleges violate the GLBA and the Safeguarding Rule.

## The Settlement

The settlement—which is not final and is available for public comment—will result in a consent decree if finalized. That consent decree enjoins certain prohibited practices and imposes significant reporting and record-keeping requirements, as well as a requirement that Venmo obtain biennial assessments of its privacy and security practices and report the results to the FTC.

## The Key Take-aways

The settlement offers lessons to any financial institution. The key ones are these:

- A financial institution—or any other company—purchasing a company should ensure that after the purchase the acquired company is complying with all legal obligations. Many financial institutions are part of large corporate families, and often grow by acquisition. It is critical to understand whether an acquired business is in compliance with privacy and security requirements, and whether its practices are consistent with disclosures about those practices.
- Disclosures to the public about privacy practices must be completely accurate and must be clear and conspicuous. Conduct that may not otherwise violate the GLBA may lead to liability under Section 5 of the Federal Trade Act if the company's privacy notices and disclosures are not accurate.
- Financial institutions should give serious consideration to "privacy by design" concepts. Venmo might have avoided much of its privacy problems had privacy been the default, with consumers left to take affirmative steps to make their transactions public, rather than the other way around. Privacy settings should be easy to find and easy to navigate.
- Companies must take security seriously, particularly where financial information is at issue. When companies make disclosures about security, particularly disclosures that describe their security measures as "bank grade" or "state of the art," those disclosures must be true. Financial institutions should regularly review their disclosures against their actual practices to ensure that disclosures that may have been accurate when drafted remain accurate in light of current practices.