AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2018
VOL. 4 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 9 | NOVEMBER-DECEMBER 2018

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [281] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Four Years Later, FTC Continues to Challenge Misleading Marketing and Privacy Practices

By Stephen E. Reynolds, Martha Kohlstrand, and Mason Clark*

The Federal Trade Commission unanimously approved a settlement with PayPal, Inc., after PayPal's peer-to-peer payment service app, Venmo, allegedly deceived users about its privacy practices, security controls, and fund transfer policies. The authors of this article discuss the settlement.

The Federal Trade Commission ("FTC") can take action to hold your company accountable for promises made in privacy notices. Venmo recently learned the hard way that the FTC remains committed to that goal.

The FTC unanimously approved a settlement with PayPal, Inc., after PayPal's peer-to-peer payment service app, Venmo, allegedly deceived users about its privacy practices, security controls, and fund transfer policies.[1] Accessible on smart devices and free of charge, Venmo is a convenient and inexpensive service to pay rent or split the check.[2] But in light of the FTC's investigation, companies should closely re-examine their privacy statements and security procedures.

THE FTC TARGETS MISLEADING MARKETING STATEMENTS AND PRIVACY SETTINGS

According to the complaint, Venmo notified users when funds were available for transfer to an external bank account, but failed to tell users the funds could be frozen or removed subject to the app's review of the transaction for fraud or other suspicious activity.[3] The FTC found Venmo's review process particularly troubling, because the app marketed overnight transfers or transfers "in as little as one business day," even though they were fully aware of mounting consumer complaints about delayed or declined transfers.[4]

---

* Stephen E. Reynolds (stephen.reynolds@icemiller.com), a former computer programmer and IT analyst, is a partner in Ice Miller's Litigation Group and co-chair of the firm's Data Security and Privacy Practice. Martha Kohlstrand (martha.kohlstrand@icemiller.com) is an associate in the firm's Litigation Group focusing much of her work on data protection and privacy issues. Mason Clark was a summer clerk at the firm.

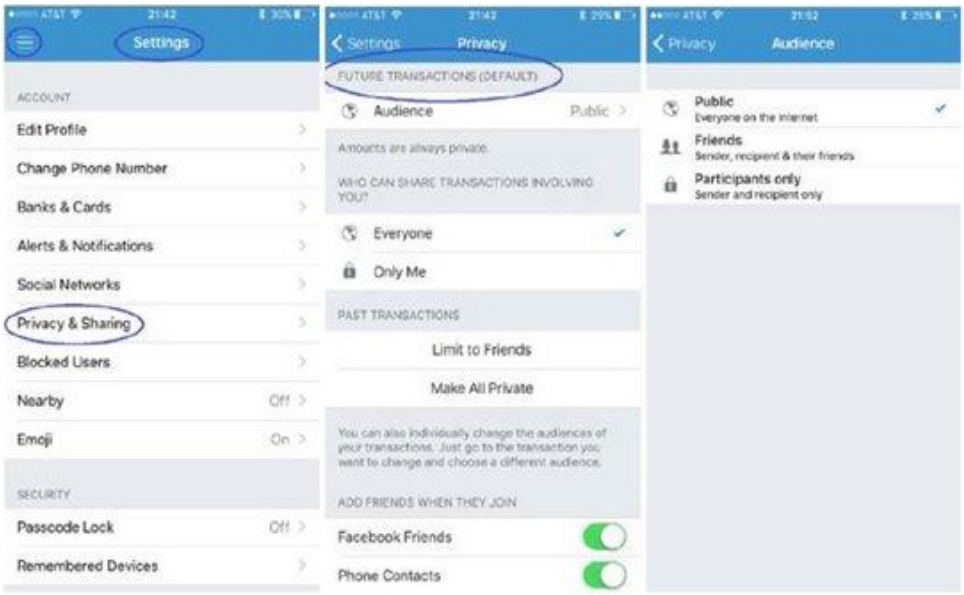
[1] *PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act*. Fed. Trade. Comm'n, https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

[2] Cochrane, Matthew, *Venmo Me: PayPal Takes Its Popular App to the Next Level,* The Motley Fool (Nov. 14, 2017), https://www.fool.com/investing/2017/11/14/venmo-me-paypal-takes-its-popular-app-to-the-next.aspx.

[3] *In the Matter of PayPal, Inc.* ("Complaint"). Fed Trade. Comm'n, https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter.

[4] *Id.* at ¶ 11-15.

Venmo's privacy settings also allegedly misled users. The app allows users to share their purchases publicly on the app's social news feed, but also permits users to limit their "default audience" privacy setting. The FTC stated the setting made users believe that limiting the default audience setting to "Participants Only" would keep transactions private regardless of whether the participant sent or received payment. Instead, the consumer also has to change a *second* setting below the default audience option, as depicted below and in the Complaint, and must select "Only Me" under the second privacy setting.[5] Allegedly, Venmo did not adequately disclose this procedure to consumers and misrepresented what steps were necessary to keep transactions private.



Marketing a product well sometimes requires risk-taking and boundary-pushing. But crossing the line between clever and deceptive carries dangerous consequences for your business. Financial damages to users resulting from marketing statements that may be viewed as deceptive provide tangible evidence of harm. Similarly, unclear or difficult privacy procedures may confuse consumers and draw the ire of the FTC.

INFORMATION SECURITY PRACTICES MUST BE ACCURATELY REPRESENTED

According to the Complaint, Venmo also made untruthful public statements on its website and app about its information security principles. For example, the app stated Venmo "uses bank-grade security systems and data encryption to protect your financial

[5] *Id.* at ¶ 20-21.

information" and prevents unauthorized transactions or access to personal information, which allegedly turned out to be inaccurate.[6] According to the Complaint, until March 2015, Venmo lacked sufficient security practices to protect user confidentiality and even failed to notify customers when their email addresses/passwords were changed and new devices were added to the account. Both scenarios allegedly led to successful hacks of user accounts.[7]

FINANCIAL INSTITUTIONS' PRIVACY PRACTICES MUST COMPLY WITH THE GRAMM-LEACH-BLILEY ACT

The Gramm-Leach-Bliley Act ("GLBA")[8] is a federal law that requires "financial institutions" to provide accurate, clear, and conspicuous notice of its privacy practices (the "Privacy Rule")[9] and establish safeguards that keep customers' personal information safe and confidential (the "Safeguards Rule").[10] Because Venmo is a financial institution, it must comply with the GLBA.

Under the Privacy Rule, Venmo must provide users with a *clear and conspicuous* initial privacy notice that accurately reflects the app's privacy practices, and the notice must be provided so users can reasonably be expected to receive notice. The FTC found the app's privacy policy, hyperlinked in grey text on a grey background in much smaller font than the rest of the app's text, was unclear to the reasonable user.[11] Furthermore, the FTC concluded that the privacy statement failed the second and third Privacy Rule requirements, because it is inaccurate and does not require receipt by the user before acceptance of the service. Yes, Venmo provides a link for customers to visit the privacy policy, but they can create a Venmo account without receiving it.[12]

The FTC also alleged that Venmo violated the Safeguards Rule, which requires companies to assess and address the risks to customer information in all areas of their operation. The Rule requires companies to develop a written information security plan that describes their programs to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. Through August 2014, the app had no written security program; until September 2014, the app failed to address reasonably foreseeable internal and external security concerns; and until March 2015,

[6] *Id.* at ¶ 32.
[7] *Id.* at ¶ 33.
[8] Also known as the Financial Services Modernization Act of 1999, Public Law 106-102, 113 Stat. 1338 (enacted November 12, 1999).
[9] Privacy of Consumer Financial Information Rule, 16 C.F.R. Pt. 313.
[10] Standards for Safeguarding Customer Information, 16 C.F.R. Pt. 314.
[11] *Id.* at ¶ 38.
[12] *Id.*

the app failed to implement basic safeguards – such as security notifications and customer support – for user information.[13]

KEY TAKEAWAYS

Generally, privacy policies should be accessible and digestible for the user, and security guarantees should be accurate and effective. When selling a home, you would prefer to not say anything about the water damage in the basement, but an appraiser might sue you if you do not. Similarly, you do not want privacy policies or security notification procedures to be the first things a potential customer sees or questions, but hiding these policies or exaggerating your security practices, in violation of the GLBA, might leave you reporting biennially to the FTC for the next 10 years.[14]

Notification can sometimes be the most helpful feature of your security practices.

Preventative measures should maintain data integrity as much as possible, but breaches and unauthorized access are inevitable. Quickly communicating with your user can help reduce the damage, however, and might even reveal an error by the user and not a compromised account. If you fail to implement either or both safeguards – preventative measures and notification processes – you are setting yourself up for a privacy headache. Not only might you cause harm and frustration to the user, you risk non-compliance with the FTC and federal laws like the Gramm-Leach-Bliley Act.

[13] *Id.* at ¶ 40.

[14] *In the Matter of Paypal, Inc.* (Order at V.). Fed Trade. Comm'n, https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter.