

E-COMMERCE, CYBER, AND ELECTRONIC PAYMENT SYSTEM RISKS: LESSONS FROM PAYPAL

LAWRENCE J. TRAUTMAN*

ABSTRACT

By now, almost without exception, every business has an internet presence, and is likely engaged in e-commerce. What are the major risks perceived by those engaged in e-commerce and electronic payment systems? What potential risks, if they become reality, may cause substantial increases in operating costs or threaten the very survival of the enterprise?

This article utilizes the relevant annual report disclosures from eBay (parent of PayPal), along with other eBay and PayPal documents, as a potentially powerful teaching device. Most of the descriptive language to follow is excerpted directly from eBay's regulatory filings. My additions include weaving these materials into a logical presentation and providing supplemental sources for those who desire a deeper look (usually in my footnotes) at any particular aspect. I've sought to present a roadmap with these materials that shows eBay's struggle to optimize its business performance while navigating through a complicated maze of regulatory compliance concerns and issues involving governmental jurisdictions throughout the world. First, a brief look is provided at the SEC's disclosure requirements. Second, a description of the eBay and PayPal history and business models is presented. Next, is a discussion of risk factors: credit cards; U.S. state money transmission laws; online and mobile growth; and reliance on internet access. International issues follow, with an examination of anti-money laundering, counter-terrorist, and other potential illegal activity laws. The author estimates that PayPal's cost of accounting and legal fees and management time devoted to the discovery, examination and documentation of the perceived enterprise risk associated with e-commerce, cyber, information technology and electronic payment system risks may aggregate in the range of tens-of-millions of dollars a year. The value proposition offered here is disarmingly simple: at no out-of-pocket cost, the reader has an opportunity to invest probably less than an hour to read and reflect upon eBay and PayPal's multiple-million-dollar research, investment and documentation of perceived e-

*BA, The American University; MBA, The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Assistant Professor of Business Law and Ethics at Western Carolina University. He may be contacted at Lawrence.J.Trautman@gmail.com. The author wishes to extend particular thanks to Alvin Harrell for his assistance in the research and preparation of this article. However, all errors and omissions are my own.

commerce, cyber, IT, and electronic payment system risk. Hopefully, this will prove of value to those either interested in the rapidly changing dynamics of (1) electronic payment systems, or (2) those engaged in Internet site operations.

TABLE OF CONTENTS

I. OVERVIEW	263
Article Value Proposition	263
II. GROWTH OF ONLINE COMMERCE.....	265
III. DISCLOSURE OF MATERIAL RISKS	267
SEC Disclosure Mandate	267
IV. EBAY: THE BUSINESS MODEL	270
General.....	270
eBay’s Marketplace	271
Monetization Strategy	273
eBay’s Payments Segment.....	274
V. PAYPAL	274
General.....	274
The Increased Importance of Mobile Devices	279
Competition.....	281
VI. RISK FACTORS	282
How PayPal Views Risk	282
Use of Credit Cards.....	286
U.S. State Money Transmission Laws	287
Online and Mobile Growth Dependence	295
Reliance on Internet Access.....	296
VII. INTERNATIONAL EXPANSION.....	297
Anti-Corruption.....	300
Localization (is Expensive).....	301
PayPal On International Risk.....	301
China.....	304
VIII. AML, COUNTER-TERRORIST LAWS, & POTENTIALLY ILLEGAL ACTIVITY	304
AML and Counter-terrorist Laws	305
Focus on Potentially Illegal Activity	305
IX. CONCLUSION	306

Ed 2] *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal* 263

“In theory, Risk Factors are intended to inform investors of each firm’s deepest fears and gravest vulnerabilities”

Tom C.W. Lin¹

I. OVERVIEW

By now, almost without exception, every business has an internet presence, and is likely engaged in e-commerce. What are the major cyber risks perceived by those engaged in e-commerce and electronic payment systems? What potential risks, if they become reality, may cause substantial increases in operating costs or threaten the very survival of the enterprise?

Article Value Proposition

Elsewhere, the author has observed that “to survive, all successful entrepreneurs must become skillful at optimizing efficiency at every opportunity.”² For the year ended December 31, 2014, PayPal incurred general and administrative expense of \$482 million.³ Of this amount, a reasonable guess is that the cost of accounting and legal fees and management time devoted to the discovery, examination and documentation of the perceived enterprise risk associated with e-commerce, cyber, information technology and electronic payment system risks may aggregate in the range of tens-of-millions of dollars a year. The value proposition offered here is disarmingly simple – at no out-of-pocket cost, the reader has an opportunity to invest probably less than an hour to read and reflect upon eBay and PayPal’s multiple-million-dollar research, investment and documentation of perceived e-commerce, cyber, IT, and electronic payment system risk.

Words are powerful and have meaning. This article utilizes the relevant annual report disclosures from eBay (parent of PayPal), along with other eBay and PayPal documents, as a potentially powerful teaching device. Most of the descriptive language to follow is excerpted directly from eBay’s regulatory filings. My additions include weaving these materials into a logical presentation and providing supplemental sources for those who desire a deeper look (usually in my footnotes) at any particular aspect. I’ve sought to present a roadmap with

¹ See Tom C. W. Lin, *A Behavioral Framework for Securities Risk*, 34 SEATTLE U. L. REV. 325, 329 (2011), available at <http://ssrn.com/abstract=2040946>.

² See Lawrence J. Trautman, Anthony Luppino & Malika S. Simmons, *Some Key Things U.S. Entrepreneurs Need to Know About the Law and Lawyers*, 46 TEXAS J. BUS. L. (2016), available at <http://ssrn.com/abstract=2606808>.

³ PayPal Holdings, Inc., Preliminary Information Statement dated February 25, 2015 as filed with the U.S. Sec. & Exch. Comm. on form 10 at 70, available at <https://www.sec.gov/Archives/edgar/data/1633917/000119312515062742/d877527dex991.htm> (last viewed May 30, 2015).

these materials that shows eBay's struggle to optimize its business performance while navigating through a complicated maze of regulatory compliance concerns and issues involving governmental jurisdictions throughout the world. First, a brief look is provided at the SEC's disclosure requirements. Second, a description of the eBay and PayPal history and business models is presented. Next, is a discussion of risk factors: credit cards; U.S. state money transmission laws; online and mobile growth; and reliance on internet access. International issues follow, with an examination of anti-money laundering, counter-terrorist, and other potential illegal activity laws.

The Internet, e-commerce, cyberthreats, and new mobile platforms and technology are having a major impact on payment systems and entrepreneurial business. PayPal incurs considerable management and legal expense to examine, analyze, and describe their information technology and e-commerce risk. By providing a close examination of PayPal's disclosure language, this article will hopefully prove of value to those readers interested in the rapidly changing dynamics of (1) electronic payment systems, or (2) those engaged in Internet site operations.

While a twenty-something year old MBA business school student in Washington, D.C., I was fortunate to have a part-time job abstracting and indexing SEC filings (10-Ks, 8-Ks, etc.) under a contract with the U.S. Securities and Exchange Commission (SEC). This experience provided me with substantial practice in the review and analysis of corporate financial statements. A few years later, my early career training as a securities analyst and later as an investment banker in New York City at Donaldson, Lufkin & Jenrette provided an intimate familiarity with the examination and analysis of corporate filings made by corporate securities issuers with the SEC. Recently, as I was reading eBay's annual report filed with the SEC on Form-10K, I realized that the massive document (approximately 150 pages when financial statements are included) provides an excellent insight into payment systems considerations and new challenges facing eBay as electronic commerce and payment platforms attempt to accommodate rapid changes in mobile computing and device platforms.

For some readers this article may appear to lack the customary structure, look and feel of the typical law or business school academic journal article. If this bothers you, then this article was not written for you. In an earlier draft, more than one commentator asked whether I could just paraphrase some of the heavy quotes of relevant eBay and PayPal language. If this is your reaction, you entirely miss the point. My entire purpose in crafting this article is to repackage PayPal's language (without my heavy paraphrasing) so that entrepreneurs and others interested may benefit from the considerable thought and expense devoted by those closest to the situation (under penalty of disclosure liability) to telling their story. My goal is to provide meaningful scholarly impact for individuals who either now or soon will be creating jobs in growing businesses with valuable

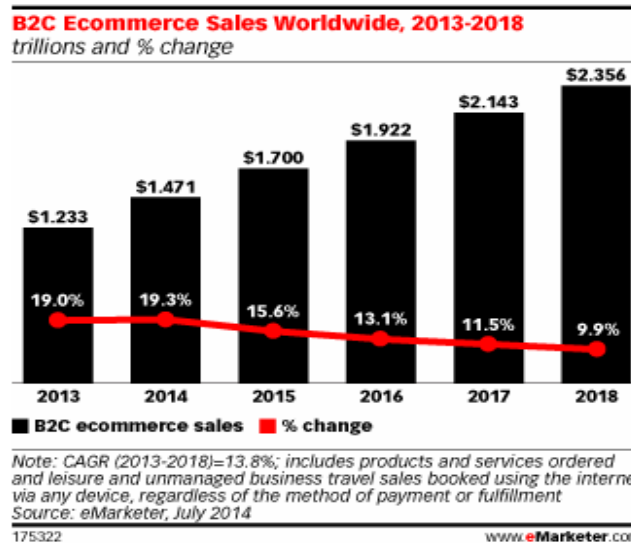
Ed 2] *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal* 265

lessons in cyber-domain risks in a highly readable manner and at no out-of-pocket cost.

II. GROWTH OF ONLINE COMMERCE

By now, everyone should understand that the continued growth of the Internet has resulted in commensurate growth in e-commerce. eMarketer reports that global e-commerce business-to-consumer (B2C) sales for 2014 will total \$1.471 trillion.⁴ Exhibit One shows that sales are expected to reach \$2.356 trillion for year 2018, and “a 10% growth rate still represents more than \$200 billion new dollars that year.”⁵

Exhibit One
Estimated Sales Growth for Worldwide Ecommerce Sales



With continued worldwide maturity of Internet usage, growth in e-commerce is expected to slow over time.⁶ However, as shown by Exhibit Two, the United States and Canada combined (North America) accounts for about a third of all worldwide dollar sales volume, and remains the leading B2C region in e-commerce sales until 2015.⁷ Note the growth of the Asia-Pacific region by 2018.

⁴ eMarketer, *Worldwide Ecommerce Sales to Increase Nearly 20% in 2014*, (July 23, 2014), available at <http://www.emarketer.com/Articles/Print.aspx?R=1011039>.

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

Exhibit Two
Regional Worldwide B2C Sales Share, 2013-2018

**B2C Ecommerce Sales Share Worldwide, by Region,
2013-2018**
% of total

	2013	2014	2015	2016	2017	2018
North America	34.9%	32.9%	31.7%	31.1%	30.7%	30.6%
Asia-Pacific	28.3%	31.2%	33.4%	35.1%	36.4%	37.4%
Western Europe	26.4%	25.4%	24.6%	23.9%	23.3%	22.7%
Latin America	4.2%	4.3%	4.2%	4.1%	3.9%	3.7%
Central & Eastern Europe	4.1%	4.0%	3.8%	3.5%	3.3%	3.2%
Middle East & Africa	2.2%	2.3%	2.3%	2.4%	2.4%	2.5%

Note: includes products and services ordered and leisure and unmanaged business travel sales booked using the internet via any device, regardless of the method of payment or fulfillment; numbers may not add up to 100% due to rounding
Source: eMarketer, July 2014

175334 www.eMarketer.com

Professor David Evans describes an “attention market,” where marketing efforts are focused on attracting “the attention of people and then sell advertisers access to that attention. The scarcity of attention –there’s only 24 hours in a day and much of that is spoken for –result in intense competition for people’s time and incentives to develop creative ways to people’s attention.”⁸ Elsewhere, Professor Evans observes that, “Multi-sided platforms such as exchanges, search engines, social networks and software platforms create value by assembling and serving communities of people and businesses. They generally come into being to solve a transaction problem that prevents agents from getting together to exchange value.”⁹ In addition

Multi-sided platform markets have two or more different groups of customers that businesses have to get and keep on board to succeed. These industries range from dating clubs (men and women), to video game consoles (game developers and users), to payment cards (cardholders and merchants), to operating system software (application developers and users). They include some of the most important industries in the economy. A survey of businesses in these industries shows that multi-sided platform businesses devise entry strategies to get multiple sides of the market on board and devise pricing, product, and other

⁸ See David S. Evans, *Rivals for Attention: How Competition for Scarce Time Drove the Web Revolution, What it Means for the Mobile Revolution, and the Future of Advertising*, 1 (2014), available at <http://ssrn.com/abstract=2391833>.

⁹ See David S. Evans, *Governing Bad Behavior by Users of Multi-Sided Platforms*, 2 BERKELEY TECH. L.J. (Fall 2012), available at <http://ssrn.com/abstract=1950474>.

competitive strategies to keep multiple customer groups on a common platform that internalizes externalities across members of these groups.¹⁰

To become successful with multi-sided platforms, Entrepreneurs “must secure enough customers on both sides, and in the right proportions, to provide enough value to either group of customers and to achieve sustainable growth. In particular, these entrepreneurs must secure ‘critical mass’ to ignite the growth of their platforms. . . [otherwise] implosion of the platform [results].”¹¹ While the competition in the financial services industry remains intense, some suggest that “ultimately, the growth of national bank brands, technological developments, and innovative business models are likely to independently result in a radical reshaping of the payments world that will ease merchant-bank tensions, but also blur the distinction between banking and commerce.”¹²

III. DISCLOSURE OF MATERIAL RISKS

SEC Disclosure Mandate

Professor Stephen Bainbridge observes that “Mandatory disclosure is a— if not the—defining characteristic of U.S. securities regulation.¹³ Congress intended the securities laws to “substitute a philosophy of full disclosure for the

¹⁰ See David S. Evans, *Some Empirical Aspects of Multi-sided Platform Industries*, 2 REV. NETWORK ECON. 191 (2003), available at <http://ssrn.com/abstract=447981>.

¹¹ See David S. Evans, *How Catalysts Ignite: The Economics of Platform-Based Start-Ups. PLATFORMS, MARKETS AND INNOVATION*, (A. Gawer, ed., Cheltenham, UK and Northampton, MA, US: Edward Elgar) (2009), available at <http://ssrn.com/abstract=1279631>. See also David S. Evans, *The Web Economy, Two-Sided Markets and Competition Policy* (2010), available at <http://ssrn.com/abstract=1584363>; David S. Evans & Richard Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses*, In Roger Blair and Daniel Sokol, eds., *Oxford Handbook on International Antitrust Economics*, Oxford University Press (2014), available at <http://ssrn.com/abstract=2185373>; David S. Evans, Richard Schmalensee, Michael D. Noel, Howard H. Chang & Daniel D. Garcia-Swartz, *Platform Economics: Essays on Multi-Sided Businesses*, In *PLATFORM ECONOMICS: ESSAYS ON MULTI-SIDED BUSINESSES*, (David S. Evans, ed., Competition Policy International) (2011), available at <http://ssrn.com/abstract=1974020>.

¹² See Adam J. Levitin, *Payment Wars: The Merchant-Bank Struggle for Control of Payment Systems*, 12 STAN. J.L. BUS. & FIN. (2007), available at <http://ssrn.com/abstract=981637>.

¹³ See Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023 (2000), available at <http://ssrn.com/abstract=329880>, citing *Europe & Overseas Commodity Traders, S.A. v. Banque Paribas London*, 147 F.3d 118, 126 (2d Cir. 1998) (“Through mandatory disclosure, Congress sought to promote informed investing and to deter the kind of fraudulent salesmanship that was believed to have led to the market collapse of 1929.”). See also Lawrence J. Trautman & George Michaely, *The SEC & The Internet: Regulating the Web of Deceit*, 68 THE CONSUMER FIN. L.Q. REP. 262 (2015), available at <http://www.ssrn.com/abstract=1951148>.

philosophy of caveat emptor”¹⁴ “Since the Depression, the Securities and Exchange Commission’s totemic philosophy has been to promote a robust informational foundation for private decision makers, thereby furthering efficiency and corporate governance,” observes Henry T.C. Hu, the inaugural Director of the Division of Risk, Strategy, and Financial Innovation of the U.S. Securities and Exchange Commission (2009-2011).¹⁵ Therefore, disclosure of all material facts by issuers of securities offered or trading in the United States is the principle at the foundation of federal securities regulation enforced by the U.S. Securities and Exchange Commission by virtue of the Securities Act of 1933¹⁶ (the Securities Act) and the Securities Exchange Act of 1934 (the Exchange Act),¹⁷ SEC Commissioner Troy A. Paredes observes that “for nearly 80 years, the SEC’s signature mandate has been to use disclosure to promote transparency,”¹⁸ as envisioned by President Roosevelt in his March 29, 1933 message to Congress when he said

There is . . . An obligation upon us to insist that every issue of new securities to be sold in interstate commerce shall be accompanied by full publicity and information, and that no essentially important element attending the issue shall be concealed from the buying public. The proposal adds to the ancient rule of caveat emptor, the further doctrine, “let the seller also beware.” It puts the burden of telling the whole truth on the seller. It should give impetus to honest dealing in securities and thereby bring back public confidence.¹⁹

¹⁴ See Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023 (2000), available at <http://ssrn.com/abstract=329880>, citing *SEC v. Capital Gains Research Bureau, Inc.*, 375 U.S. 180, 186 (1963).

¹⁵ See Henry T.C. Hu, *Too Complex to Depict? Innovation, ‘Pure Information,’ and the SEC Disclosure Paradigm*, 90 TEX. L. REV. 1601 (2012), available at <http://ssrn.com/abstract=2083708>.

¹⁶ 15 U.S.C. §§77a-aa (2000).

¹⁷ *Id.* §§78a-nn. See also John C. Coffee, *The Future as History: The Prospects for Global Convergence in Corporate Governance and Its Implications* (February 1999), Columbia Law Sch. Center for Law and Econ. Stud. Working Paper No. 144, available at: <http://ssrn.com/abstract=142833>.

¹⁸ See Troy A. Paredes, Commissioner U.S. Securities and Exchange Commission, Remarks at The SEC Speaks 2013 (Feb. 22, 2013), available at <http://www.sec.gov/news/speech/2013/spch022213tap.htm>; Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023-1060, (2000), available at: <http://ssrn.com/abstract=329880>.

¹⁹ See Paredes, *supra* note 18 citing S. Rep. No. 73-47, at 6-7 (1933) & H.R. Rep. No. 73-85, at 1-2 (1933). See also Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023 (2000); Lucien A. Bebchuk, Alma Cohen & Allen Farrell, *What Matters Most in Corporate Governance?*, 22 REV. FIN. STUD. 783 (2009).

Ed 2] *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal* 269

Beginning in 2005, the SEC “required all firms to include a new section in their annual filings (Section 1A of the Annual Report on Form 10-K) to discuss ‘the most significant factors that make the company speculative or risky’ (Regulation S-K, Item 305(c), SEC 2005).”²⁰ According to Professor Tom C.W. Lin

The objective of the Securities Act is to ensure ‘full and fair disclosure of the character of securities sold in interstate and foreign commerce and through the mails, and to prevent frauds in the sale thereof...Pursuant to its mandated registration process and its antifraud provisions, the Securities Act attempts to ensure that investors receive accurate and meaningful information about the offered securities and their issuing firms. The Exchange Act, in turn, governs the subsequent trading of those securities in secondary markets. Like the Securities Act, the Exchange Act attempts to ensure that investors in those secondary markets receive accurate and meaningful information about the offered securities and their issuing firms. The Exchange Act works to achieve this purpose by requiring periodic reporting filings and by imposing a broad anti-fraud provision in Section 10.²¹

Fast forward a few years and the United States undergoes a traumatic meltdown of its financial markets during 2008 and 2009. Professor Hu contends that the SEC’s disclosure philosophy

[H]as always been substantially implemented through what can be conceptualized as an ‘intermediary depiction’ model. An intermediary—e.g., a corporation issuing shares—stands between the investor and an objective reality. The intermediary observes that reality, crafts a depiction of the reality’s pertinent aspects, and transmits the depiction to investors. Securities law directs that

²⁰ See John L Campbell, Hsinchun Chen, Dan S. Dhaliwal, Hsin-min Lu, and Logan B Steele, *The Information Content of Mandatory Risk Factor Disclosures in Corporate Filings*, REV. ACCT. STUD. 1 (Forthcoming) available at <http://ssrn.com/abstract=1694279>.

²¹ See Lin, *supra* note 1 at 329; Stephen J. Brown, William N. Goetzmann, Bing Liang, & Christopher Schwarz, *Mandatory Disclosure and Operational Risk: Evidence from Hedge Fund Registration*, J. FIN. (Forthcoming); Yale ICF Working Paper No. 06-15, available at <http://ssrn.com/abstract=918461>; Scott E. Coull, & Erin E. Kenneally, *A Qualitative Risk Assessment Framework for Sharing Computer Network Data* (March 31, 2012). 2012 TRPC. available at <http://ssrn.com/abstract=2032315>; Todd D. Kravet & Volkan Muslu, *Textual Risk Disclosures and Investors’ Risk Perceptions* (June 2, 2012). REV. ACCT. STUD. (Forthcoming), available at: <http://ssrn.com/abstract=1736228>; But see Simon C.Y. Wong, *A Call to Reform US Disclosure-Based Regulation*, BUTTERWORTHS J. INT’L BANKING & FIN. L. 77, (Feb. 2010); Northwestern Law & Econ. Research Paper No. 10-07, available at <http://ssrn.com/abstract=1556542>.

depictions are to be accurate and complete. ‘Information’ is conceived of in terms of, if not equated to, such depictions...²²

Professor Hu argues that “Modern financial innovation has resulted in objective realities that are far more complex than in the past, often beyond the capacity of the English language, accounting terminology, visual display, risk measurement, and other tools on which all depictions must primarily rely.”²³ Of particular importance to this inquiry, Professor Lin observes that “in theory, Risk Factors are intended to inform investors of each firm’s deepest fears and gravest vulnerabilities.”²⁴ David Larcker and Brian Tayan describe *risk management* as “the process by which a company evaluates and reduces its risk exposure. This includes actions, policies, and procedures that management implements to reduce the likelihood and severity of adverse outcomes and to increase the likelihood and benefits of positive outcomes.”²⁵ How eBay (PayPal) perceives its greatest threat of risk is explored in the following pages.

IV. EBAY: THE BUSINESS MODEL

General

eBay Inc., incorporated in California during May 1996 and parent of PayPal, describes itself as a “global technology company that enables commerce through three reportable [business] segments: Marketplaces, Payments, and GSI [the commerce and interactive marketing services provider purchased in June 2011]...”²⁶ Moreover, eBay suggests that it is able to facilitate transactions “by providing online platforms, tools and services to help individuals and small,

²² See Hu, *supra* note 15 at 1601. See generally Lawrence J. Trautman, Personal Ethics & the U.S. Financial Collapse of 2007-08, (forthcoming), available at <http://ssrn.com/abstract=2502124>.

²³ *Id.*, See also Steven L. Schwarcz, *Rethinking the Disclosure Paradigm in a World of Complexity*, U. ILL. L. REV. (2004), available at: <http://ssrn.com/abstract=336685>; Joseph A. Grundfest, *The Future of United States Securities Regulation in an Age of Technological Uncertainty*, Stanford Law & Econ. Olin Working Paper No. 210 (2000), available at <http://ssrn.com/abstract=253763>.

²⁴ See Lin, *supra* note 1 at 330; Lucian A. Bebchuk, Alma Cohen & Allen Ferrell, *What Matters in Corporate Governance?*, 22 REV. FIN. STUD. 783, (Feb. 2009), available at <http://ssrn.com/abstract=593423>.

²⁵ See David Larcker & Brian Tayan, CORPORATE GOVERNANCE MATTERS: A CLOSER LOOK AT ORGANIZATIONAL CHOICES AND THEIR CONSEQUENCES 190 (Pearson 2011).

²⁶ See Form 10-K (Annual Report) for eBay Inc., for the Fiscal Year ended Dec. 31, 2012, 4 available at http://www.sec.gov/Archives/edgar/data/1065088/000106508813000004/ebay2012_10k.htm.

Ed 2] *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal* 271

medium and large merchants around the globe engage in online and mobile commerce and payments.”²⁷

eBay’s Marketplace

Buyers and sellers of new and second-hand goods are brought together by eBay’s online marketplace. Contracts between buyers and sellers (eBay “members”) are formed; however, eBay itself is not a party to the sales contract.²⁸ Selby and Manning state that “eBay’s business model is predicated upon its ability [to] capture a proportion of the value it generates for its Members by lowering their transaction costs as compared to its competitor auction sites, both off-line and on-line.”²⁹ The development of cultural norms and “community” also appears to be a unique attribute of eBay’s marketplace, “including a culture of freedom of contract between Members and that eBay is a community which is heavily dependent upon trust between members. eBay has even recognized this cultural norm in its User Agreement with its Members...”³⁰ eBay’s “Disclaimer of Warranties and Limitation of Liability” language from its User Agreement posted April 26, 2013 is reproduced below as follows:

Disclaimer of Warranties; Limitation of Liability

We try to keep eBay and its sites, services, applications, and tools safe, secure, and functioning properly. You acknowledge that we cannot guarantee the continuous operation of or access to our sites, services, applications, or tools. You further acknowledge that operation of and access to our sites, services, applications, or tools may be interfered with as a result of technical issues or numerous factors outside of our control. Bid updates and other notification functionality in eBay’s applications may not occur in real time. Such functionality is subject to delays including, without limitation, delays, or latency due to your physical location or your wireless

²⁷ *Id.* at 4. See also Elizabeth Brown & Inara Scott, I Do Not Think It Means What You Think It Means: Redefining and Regulating the Sharing Economy, (paper presented at 2016 Academy of Legal Studies in Business Annual Conference) (forthcoming); Robin Sickles & Kevin Hasker, *eBay in the Economic Literature: Analysis of an Auction Marketplace*, 37 REV. INDUSTRIAL ORGANIZATION 3 (2010); Robin Sickles, Kevin Hasker & Bibo Jiang, Estimating Consumer Surplus in e-Bay Computer Monitor Auctions, Chapter 4 of Festschrift in Honor of Peter Schmidt: Econometric Methods and Applications. R.C Sickles and WC Horrace (eds.) Springer Science & Business Media, New York, NY, 83-102, (2014); Abbey Stemler, The Myth of the Sharing Economy and Its Implications for Regulating Innovation (forthcoming), available at <http://ssrn.com/abstract=2828308>.

²⁸ See John E. Selby & Christopher J. Manning, *eBay’s Paypal: Balancing Marketplace and Regulatory Regimes*, 6 COMPUTER L. REV. INT’L 168, 169 (2008), available at <http://ssrn.com/abstract=1352083>.

²⁹ *Id.* at 168.

³⁰ *Id.*

data service provider's network. You agree that you are making use of our sites, services, applications, and tools at your own risk, and that they are being provided to you on an "AS IS" and "AS AVAILABLE" basis. Accordingly, to the extent permitted by applicable law, we exclude all express or implied warranties, terms and conditions including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

In addition, to the extent permitted by applicable law, we are not liable, and you agree not to hold eBay responsible, for any damages or losses (including, but not limited to, loss of money, goodwill or reputation, profits, or other intangible losses or any special, indirect, or consequential damages) resulting directly or indirectly from:

- Your use of or your inability to use our sites, services and tools;
- Delays or disruptions in our sites, services, applications, or tools;
- Viruses or other malicious software obtained by accessing our sites, services, applications, or tools or any site, services, applications, or tools linked to our sites, services, applications, or tools;
- Glitches, bugs, errors, or inaccuracies of any kind in our sites, services, applications, and tools or in the information and graphics obtained from them;
- Damage to your hardware device(s) or loss of data that results from the use of our sites, services, applications, and tools;
- The content, actions, or inactions of third parties, including items listed using our sites, services, applications, or tools, feedback provided by third parties, or the destruction of allegedly fake items;
- A suspension or other action taken with respect to your account;
- The duration or manner in which your listings appear in search results as set forth in the Listing Conditions Section below;
- eBay's decision to end or remove your listing(s);
- Your need to modify practices, content, or behavior or your loss of or inability to do business, as a result of changes to this User Agreement or our policies; eBay reserves the right to modify its policies and this User Agreement at any time consistent with the provisions outlined herein.

Some jurisdictions do not allow the disclaimer of warranties or exclusion of damages, so such disclaimers and exclusions may not apply to you.

You acknowledge that we are not a traditional auctioneer. Instead, our sites are venues to allow users to offer, sell, and buy just about anything, at

any time, from anywhere, in a variety of pricing formats and locations, such as Stores, fixed price formats and auction-style formats. We are not involved in the actual transaction between buyers and sellers. Any pricing, shipping or other guidance we provide in our sites, services, applications, or tools is solely informational and you may choose not to follow such guidance at any time. We do not warrant or guarantee that any particular results will be achieved from following guidance we provide (e.g. that your listing will sell, that a particular shipping option is the least expensive, etc.) While we may help facilitate the resolution of disputes through various programs, we have no control over and do not guarantee the existence, quality, safety, or legality of items advertised; the truth or accuracy of users' content or listings; the ability of sellers to sell items; the ability of buyers to pay for items; or that a buyer or seller will actually complete a transaction or return an item.

Regardless of the previous paragraphs, if we are found to be liable, our liability to you or to any third party is limited to the greater of (a) any amounts due under the eBay Buyer Protection Policy up to the price the item sold for on eBay (including any applicable sales tax) and its original shipping costs, (b) the amount of fees in dispute not to exceed the total fees, which you paid to us in the 12 months prior to the action giving rise to the liability, or (c) \$100.³¹

Monetization Strategy

Whether online, through the mobile channel or offline, our monetization strategy remains the same. We are primarily a transaction-based business model that generates revenue through our commerce and payments platforms. We also generate revenue through marketing services, classifieds and advertising. As of December 31, 2012, [eBay's] Marketplaces platforms (which bring consumers and merchants together through online websites and mobile applications that are generally available throughout the world at any time, including through localized eBay.com sites in many countries) had more than 112 million active users and more than 350 million listings globally, while [the] Payments segment had more than 122 million active registered accounts. A user may have more than one account

³¹ eBay User Agreement (Posted Apr. 26, 2013. Effective for new users immediately and for current users on July 1, 2013 and superseding all previous versions of the eBay User Agreement), available at <http://pages.ebay.com/help/policies/user-agreement.html?rt=nc> (last viewed Aug. 25, 2015). *But see* Miriam Albert, E-Buyer Beware: Why Online Auction Fraud Should Be Regulated, 39 AM. BUS. L.J. 575 (2002), available at <http://ssrn.com/abstract=1676905> (describing online auction fraud as the most commonly reported form of Internet fraud).

on our Marketplaces trading platforms and therefore may be counted more than once when we calculate the number of active users...³²

eBay's Payments Segment

Our Payments segment has three primary payments brands: PayPal, which enables individuals and businesses to securely, easily and quickly send and receive payments online and through a broad range of mobile devices in approximately 190 markets worldwide; Bill Me Later, which enables U.S. merchants to offer, and U.S. consumers to obtain, credit at the point of sale for ecommerce and mobile transactions through Bill Me Later's relationship with a chartered financial institution; and Zong, acquired in August 2011, which enables users with a mobile phone to purchase digital goods and have the transactions charged to their phone bill. In 2011, we also acquired BillsAFE, a provider of payment services for online merchants in Germany that offer consumers the ability to pay for purchases upon receipt of an invoice after the item is received.³³

V. PAYPAL

General

PayPal is headquartered in San Jose, California, and is the eBay online payments platform located at www.paypal.com and its localized counterparts.³⁴ eBay purchased PayPal during 2002, "because it was more popular with buyers and sellers on eBay marketplace than eBay's own payment systems service."³⁵ In September 2014, eBay, Inc. announced the planned separation of eBay and PayPal into independent publicly-traded companies in the third quarter of 2015.³⁶

As shown in Exhibit One, the Company discloses that as of the first-Quarter, 2015, PayPal has "165 million active registered accounts and supports payments in 100 currencies...[And] has localized marketing websites in more than 80 markets around the world."³⁷

³² eBay Form 10-K *supra* note 26 at 4.

³³ eBay Form 10-K *supra* note 26 at 6. See also Hal S. Scott, The Importance of the Retail Payment System, (2014), available at <http://ssrn.com/abstract=2539150>.

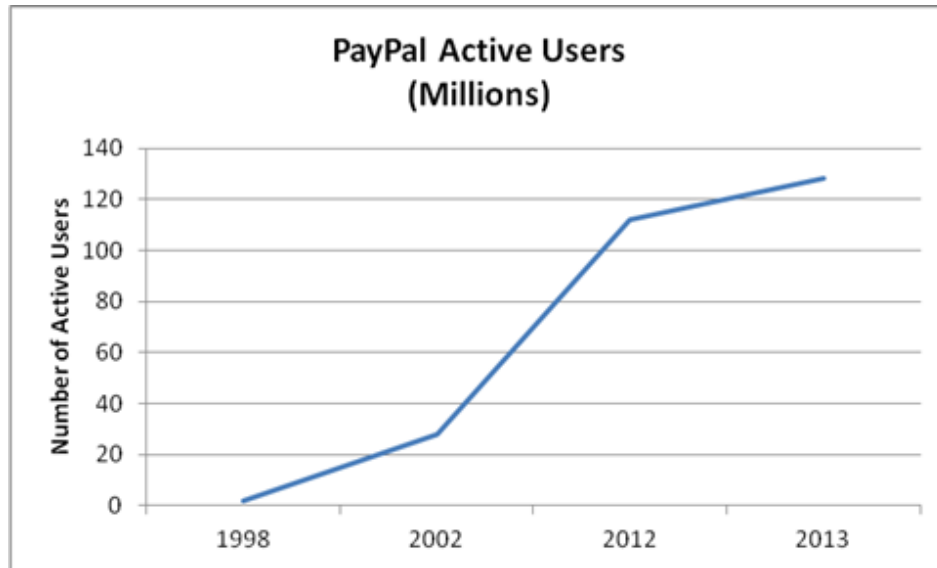
³⁴ *Id.* at 4.

³⁵ See Selby & Manning, *supra* note 28 at 168, citing Margaret Kane, *eBay Picks Up PayPal for \$1.5 Billion*, (2002) CNet News, <http://news.cnet.com/2100-1017-941964.html> (last viewed Aug. 25, 2015).

³⁶ PayPal Q1 2015 Fact Sheet, available at https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_Q1_2015_Fast_Facts.pdf (last viewed Aug. 25, 2015).

³⁷ PayPal, Q1 2013 FAST FACTS, available at https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_Q1_2013_Fast_Facts.pdf. (last viewed Sept. 4, 2016).

Exhibit Three



Source: eBay Annual Reports on Form 10-K for the periods ending December 31st, 2002, 2012, & 2013.

During the first quarter of 2013 alone, PayPal added more than 5 million active accounts.³⁸ Other financial metrics indicate that:

- PayPal revenues represented 41% of eBay Inc. revenues in Q1 2013.
- PayPal revenues for Q1 2013 were \$1.5 billion, growing 20% year over year on an FX neutral basis.
- PayPal's international business generated \$795 million in revenue in Q1 2013, and international revenue grew at a rate of 19% year over year.
- For the sixth quarter in a row, PayPal's international revenue represented more than half of PayPal's total revenue, at 51%.
- PayPal's net Total Payment Volume, the total value of transactions in Q1 2013 was \$41 billion, up 22 % year over year on an FX neutral basis.
- PayPal transacted \$5,277 in Total Payment Volume every second in Q1 2013.
- PayPal customers made 682 million transactions in Q1 2013, or 7.6 million payments per day.³⁹

³⁸ *Id.*

³⁹ *Id.*

The markets for PayPal's products and services are intensely competitive and are subject to rapid technological change, including but not limited to: mobile payments, electronic funds transfer networks allowing Internet access, cross-border access to payment networks, creation of new payment networks, and new technologies for enabling merchants, both online and offline, to process payments more simply. PayPal faces competition and potential competition from existing online, mobile and offline payment methods, including, among others:

- providers of traditional payment methods, particularly credit and debit cards, checks, money orders and Automated Clearing House transactions (these providers are primarily well-established banks);
- providers of "digital wallets" which offer customers the ability to pay online or on mobile devices through a variety of payment methods, including Visa's V.me, American Express's Serve, Google Wallet and the recently announced Merchant Customer Exchange (MCX) initiative supported by Walmart, Target and other major U.S. retailers;
- payment-card processors that offer their services to merchants, including Square, Chase Paymentech, First Data, Wells Fargo, WorldPay, Barclays Merchant Services, Global Payments, Inc., and Stripe, and payment gateways, including CyberSource and Authorize.net (both owned by Visa), Braintree and First Data;
- Amazon Payments, which offers merchants the ability to accept credit card- and bank-funded payments from Amazon's base of online and mobile customers on the merchant's own website; and
- providers of mobile payments, including ISIS in the U.S., Buyster in France, Mpass in Germany, Weve in the U.K., Boku, Venmo (acquired by Braintree) and Crandy, many of which are owned by or supported by major mobile carriers.
- providers of mobile payments, including ISIS in the U.S., Buyster in France, Mpass in Germany, Weve in the U.K., Boku, Venmo (acquired by Braintree) and Crandy, many of which are owned by or supported by major mobile carriers.

PayPal also faces competition and potential competition from:

- money remitters such as MoneyGram, Western Union, Global Payments, Inc. and Euronet;
- bill payment services, including CheckFree, a subsidiary of Fiserv;
- services that provide online merchants the ability to offer their customers the option of paying for purchases from their bank account or paying on credit, including

ClearXchange (a joint venture among Wells Fargo, Bank of America and JP Morgan Chase), Western Union's WU Pay, Dwolla, Acculynk, TeleCheck (a subsidiary of First Data), iDEAL in the Netherlands, Sofortuberweisung in Germany and the recently-announced MyBank pan-European initiative;

- issuers of stored value targeted at online payments, including NetSpend, Green Dot, PayNearMe and UKash;
- online payment-services providers such as AliPay, the PayU group of companies (owned by Naspers), PagSeguro, Bcash (owned by Naspers) and Klarna;
- other providers of online account-based payments, such as Skrill, ClickandBuy (owned by Deutsche Telekom), Barclays Pingit in the U.K., Kwixo in France, and Paymate and Visa PayClick in Australia;
- payment services targeting users of social networks and online gaming, including PlaySpan (owned by Visa), Boku and Bango;
- payment services enabling banks to offer their online banking customers the ability to send and receive payments through their bank account, including ZashPay from Fiserv and Popmoney from CashEdge (recently acquired by Fiserv), both of which have announced collaboration agreements with Visa; and
- online shopping services that provide special offers linked to a specific payment provider, such as Visa's RightCliq, MasterCard MarketPlace, TrialPay and Tapjoy.

Some of these competitors have longer operating histories, significantly greater financial, technical, marketing, customer service and other resources, greater brand recognition, or a larger base of customers than PayPal, and may be also be able to leverage other affiliated businesses for competitive advantage. PayPal's competitors may be able to innovate and respond to new or emerging technologies and changes in customer requirements faster and more effectively than PayPal. Some of these competitors may also be subject to less burdensome licensing, anti-money laundering, counter-terrorist financing and other regulatory requirements than PayPal, which is subject to additional regulations based on, among other factors, its licensure as a bank in Luxembourg. They may devote

greater resources to the development, promotion, and sale of products and services than PayPal, and they may offer lower prices. For example, Google previously has offered free payments processing on transactions in amounts proportionate to certain advertising spending with Google. We also expect new entrants, such as MCX, to offer competitive products and services. In addition, some merchants provide such services to themselves. Competing services tied to established banks and other financial institutions may offer greater liquidity and engender greater consumer confidence in the safety and efficacy of their services than PayPal. In addition, in certain countries, such as Germany, Netherlands and Australia, electronic funds transfer is a leading method of payment for both online and offline transactions. In the U.K., the Payments Council has announced that mobile payments between bank accounts will be broadly available beginning in 2014. As in the U.S., established banks and other financial institutions that do not currently offer online payments could quickly and easily develop such a service.

The principal competitive factors for PayPal include the following:

- ability to attract, retain and engage both buyers and sellers with relatively low marketing expense;
- ability to show that sellers will achieve incremental sales by offering PayPal;
- security of transactions and the ability for buyers to use PayPal without sharing their financial information with the seller;
- low fees and simplicity of fee structure;
- ability to develop services across multiple commerce channels, including mobile payments and payments at the physical point of sale;
- trust in PayPal's dispute resolution and buyer and seller protection programs;
- customer service; and
- brand recognition.

With respect to our online competition, additional competitive factors include:

- website and mobile application onboarding, ease-of-use and accessibility;
- system reliability;
- data security; and

Ed 2] *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal* 279

- quality of developer tools such as our Application Programming Interfaces and Software Development Kits.

Some of PayPal's competitors, such as Wells Fargo, First Data, American Express and Royal Bank of Scotland, also provide processing or foreign exchange services to PayPal. If PayPal were to seek to expand the financial products that it offers, either alone or through a commercial alliance or an acquisition, these processing and foreign exchange relationships could be negatively affected, or these competitors and other processors could make it more difficult for PayPal to deliver its services.⁴⁰

The Increased Importance of Mobile Devices

At the risk of stating the obvious, eBay observes that

Driven by the ubiquity of the Internet and the proliferation of mobile devices, we believe that the way consumers engage with brands and services is fundamentally changing. They are shopping virtually anytime, anywhere. We believe that this shift in behavior is blurring the lines between offline retail and online ecommerce, effectively becoming one market for commerce.⁴¹

Our Marketplaces platforms offer the following features:

PayPal provides a variety of access points for consumers to shop virtually anytime, anywhere.

Our Marketplaces platforms are accessible through a traditional online experience and from mobile devices. We offer downloadable, easy-to-use mobile applications for the iPhone, the iPad, Android and Windows mobile devices for eBay.com and some of our other websites and vertical shopping experiences, including StubHub, Fashion, Motors and Half.com. We also maintain a mobile version of our eBay.com website for use on mobile devices and continue to develop our mobile applications on an ongoing basis. In 2012, nearly \$13 billion in mobile commerce volume was

⁴⁰ eBay Form 10-K *supra* note 26 at 44.

⁴¹ *Id.* at 4.

transacted across our platforms, more than doubling our prior year's mobile commerce volume.⁴²

Our individual and merchant listings offer variety and choice.

With more than 350 million listings on all of our eBay.com platforms as of December 31, 2012, we offer consumers a broad range of listings across a wide number of categories. Our listings include new, refurbished and used products, common and rare items, and branded and unbranded products.⁴³

Our PayPal payment processing solution is available both online and on mobile devices.

PayPal started as a payment solution for online transactions between consumers and merchants through a traditional online experience. With the growth of Internet-enabled mobile devices, PayPal is becoming a popular form of payment for mobile commerce. In 2012, PayPal's net total payment volume, or net TPV, for transactions using mobile devices reached nearly \$14 billion, up from approximately \$4 billion in 2011. PayPal's mobile products are designed to deliver an end-to-end mobile shopping experience in a safe and secure environment. PayPal's mobile checkout solutions offer a convenient and easy way for merchants to accept payments from mobile devices, and for consumers to pay, through a mobile-optimized user experience. Consumers with a PayPal account have the flexibility to pay without entering a credit card number or a billing and shipping address online or through their mobile devices.

We offer consumers choice by providing a variety of funding mechanisms.

Consumers can fund their PayPal accounts and payments using PayPal in a variety of ways, including by credit card, debit card, electronic funds transfers from their bank account and through a PayPal balance if the buyer has previously received payments through PayPal or chosen to pre-fund a balance. We also provide a credit offering through our Bill Me Later service, which allows qualifying U.S. consumers to obtain a revolving line of credit at the point of sale from WebBank, a third-party chartered financial institution. Bill Me Later is not a chartered financial institution nor is it licensed to make loans in any state. Accordingly, Bill Me Later must rely on a bank or licensed lender to issue the Bill Me Later credit products and extend credit to customers. U.S. consumers may also be offered an

⁴² *Id.* at 5.

⁴³ *Id.* at 6.

opportunity to defer payments for purchases made using Bill Me Later. Under some promotional arrangements offered on select merchant sites, interest on such purchases can be deferred for as long as 18 months.⁴⁴

eBay's payments solutions offer leading fraud prevention and protection.

PayPal enables consumers to pay merchants quickly and easily without sharing sensitive financial information, such as credit card or debit card numbers. To make payments using PayPal, consumers need to disclose only their email addresses to merchants. [eBay claims that] The account-based nature of PayPal's network helps us to better detect and prevent fraud when funds enter, flow through and exit the PayPal network.

PayPal's Seller Protection Program covers sellers in certain key geographies who follow specific shipping and handling practices against claims that a transaction was not authorized by the buyer or that the item was not received. PayPal's Purchase Protection Program reimburses the buyer, subject to specified limitations, for qualified purchases using PayPal on or off eBay.com in certain key geographies if the buyer does not receive the item or, in limited markets, if the item is significantly not as described. In some non-U.S. markets, protection for buyers is limited to a maximum amount per transaction.⁴⁵

Competition

For our Payments segment, our users may choose to pay through a variety of alternative means, including credit and debit cards, automated clearing house and bank wires, other online payment services, offline payment methods such as cash, check or money order and using mobile phones. Likewise, our users may elect to finance their purchases through a broad range of other sources of financing, including credit cards, lines of credit provided by financial institutions and store credit or layaway plans provided by merchants.⁴⁶

⁴⁴ *Id.* at 7.

⁴⁵ *Id.* at 8.

⁴⁶ *Id.* at 9; See also Gary Hewitt, *Competition Issues in Electronic Commerce*, ORG. ECON. CO-OPERATION & DEV., Best Practice Roundtables in Competition Policy No. 31 (2001), available at <http://ssrn.com/abstract=318768> (Observing that the international nature of e-commerce may have heightened the need for international co-operation between competition enforcers).

VI. RISK FACTORS

How PayPal Views Risk

Corporate risk is a topic that is receiving increased focus by management and boards of directors during recent years.⁴⁷ Reports of cyber threats and data security breaches continue to grow by alarming proportions. Pinguelo and Muller “list the various forms of cybercrime as: economic or foreign espionage, malicious insiders, spamming, phishing, email extraction programs, and hacking.”⁴⁸ Professor Doris Estelle Long observes that “cyberspace is often a battlefield with a wide array of armies posed to challenge one another across the increasing array of rhetoric and technology that has made it such a potent arena for global digital commerce...”⁴⁹ In addition, “some of the lessons learned in the hard fought battles over legal protection for intellectual property in the digital world may provide guidance for the critical issues currently under discussion in the on-going efforts to establish international protection norms in the e-commerce domain.”⁵⁰ Previous articles have discussed how “few operational areas present as much inherent risk or prove as difficult to govern as Information Technology.”⁵¹

⁴⁷ See generally Chris Bronk, *Risk-Intelligent Governance in the Age of Cyberthreats* (April 29, 2013), available at <http://ssrn.com/abstract=2270853>; NAT'L ASSN. CORP. DIRS, Adv. Council on Risk Oversight: Summary of Proceedings (2012), available at http://www.nacdonline.org/files/AC%20on%20Risk%20Oversight%20Summary_Final.pdf.; Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment*, 11 FLA. ST. U. BUS. REV. 75 (2012), available at <http://www.ssrn.com/abstract=1998489>; Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. (2016), available at <http://ssrn.com/abstract=2534119>; Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, Hastings Bus. L.J. (2016), available at <http://ssrn.com/abstract=2623219>; Lawrence J. Trautman & Kara Altenbaumer-Price, *The Importance of Insurance in Managing Corporate Cyberthreat Risk*, (with Kara Altenbaumer-Price), (forthcoming);

⁴⁸ See Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Corporate Information Technology Governance Under Fire*, 8 J. STRAT. INT'L STUD. 105 (2013), available at <http://ssrn.com/abstract=2346583>. See also Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals*, 16 VA. J. L. & TECH. 116, 123-136 (2011).

⁴⁹ Doris Estelle Long, *Messages from the Front: Hard Earned Lessons on Information Security from the IP War*, 16 MICH. ST. INT'L L. REV. 71 (2007), available at: <http://ssrn.com/abstract=2223165>.

⁵⁰ *Id.*

⁵¹ See Lawrence J. Trautman & Kara & Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L., 313, 339 (2011), available at <http://www.ssrn.com/abstract=1947283>. See also Peter Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, 2 J TELECOMM. & HIGH TECH. L. 163 (2004), available at <http://ssrn.com/abstract=531782>; Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. Y POL'Y 341 (2015), available at <http://ssrn.com/abstract=2548561>; Lawrence J. Trautman, *Congressional*

All engaged in e-commerce or exposed to the use of electronic payment systems face numerous potential risks, including: cybercrime,⁵² cyberterrorism,⁵³ electronic crime, infrastructure security, intellectual property protection, internet governance,⁵⁴ jurisdictional disputes, and legal restrictions and obligations (regulations and privacy laws).⁵⁵

Cybersecurity Oversight: Who's Who & How It Works, 5 J. L. & CYBER WARFARE 147(2016); Lawrence J. Trautman, *The SONY Data Hack: Implications for World Order*, (forthcoming).

⁵² See generally Trey Herr & Sasha Romanosky, *Cyber Crime: Security Under Scarce Resources*, American Foreign Policy Council Defense Technology Program Brief, No. 11, (2015), available at <http://ssrn.com/abstract=2622683> David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine* (2015), available at <http://ssrn.com/abstract=2636944>.

⁵³ See generally Derek E., Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. (2014), available at <http://ssrn.com/abstract=2232471>; Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control* (January 28, 2012). 14 MINN. J. L., SCI. & TECH., 137, 2013 available at <http://ssrn.com/abstract=1950725>; Kelly Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent* (2009) available at <http://ssrn.com/abstract=1452803>; Jack Landman Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, U. CHI. LEGAL F., (Forthcoming) available at: <http://ssrn.com/abstract=285732>; Oren Gross, *Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. (2015), available at <http://ssrn.com/abstract=2575980>; Lene Hansen & Helen Nissenbaum, *Digital Disaster, Cyber Security and the Copenhagen School*, 53 INT'L STUD. Q. 1155 (2009), available at <http://ssrn.com/abstract=2567410>; Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L. J. (2011) available at: <http://ssrn.com/abstract=1670330>; Gregory S. McNeal, *Cyber Embargo: Countering the Internet Jihad*, 39 CASE W. RES. J. INT'L L., 789-827 (2008) available at <http://ssrn.com/abstract=1002210>; David W. Opderbeck, *Cybersecurity and Executive Power*, Seton Hall Pub. Law Research Paper No. 1788333 (2011), available at <http://ssrn.com/abstract=1788333>; Fernando M. Pinguelo & Bradford W. Muller, *Virtual Crimes – Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA J. L. & TECH. 116 (2011), available at <http://ssrn.com/abstract=1789284>; Jaroslav Sirjajev, *Cyberterrorism in the Context of Contemporary International Law*, 14 SAN DIEGO INT'L L.J. (2012), available at <http://ssrn.com/abstract=2220296>; Paul Stockton & Michele Golabek-Goldman, *Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat*, 25 STAN. L. & POL'Y REV., (2014) available at <http://ssrn.com/abstract=2257915>; Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization* (July 20, 2004), available at: <http://ssrn.com/abstract=566361>; Asaf Wiener, *Virtual Crimes, Actual Threats: Detering National Security Offenses Committed Through Cyberspace*, 4 J. L. & CYBER WARFARE (2015), available at <http://ssrn.com/abstract=2576198>.

⁵⁴ See Generally Scott Shackelford, *Gauging a Global Cybersecurity Market Failure: The Use of National Cybersecurity Strategies to Mitigate the Economic Impact of Cyber Attacks*, in *ECONOMICS OF NATIONAL CYBER SECURITY STRATEGIES* (NATO Cooperative Cyber Defence Centre of Excellence, Pascal Brangetto ed., 2015), available at <http://ssrn.com/abstract=2621754>; Scott Shackelford, *Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk*, __ CHAPMAN L. REV. (2016), available at <http://ssrn.com/abstract=2635035>; Peter Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, in *Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce*, available at <http://ssrn.com/abstract=11472>; Peter Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L L. 991 (1998), available at <http://ssrn.com/abstract=121277>; Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?*, 18 N.C. J.L. & TECH.

Among the risk factors germane to the focus of this paper that eBay's management believes may affect PayPal's operating results include:

- our ability to manage the rapid shift from online commerce and payments to mobile and multi-channel commerce and payments;
- our ability to upgrade and develop our systems infrastructure and customer service capabilities to accommodate growth and to improve the functionality and reliability of our websites and services at a reasonable cost while maintaining 24/7 operations;
- consumer confidence in the safety and security of transactions using our websites and technology (including through mobile devices) and the effect of any changes in our practices and policies or of any events on such confidence;
- our ability to comply with existing and new laws and regulations as we expand the range and geographical scope of our products and services and as we grow larger, including those laws and regulations discussed below under the caption "If our Payments business is found to be subject to or in violation of any laws or regulations, including those governing money transmission, electronic funds transfers, money laundering, terrorist financing, sanctions, consumer protection, banking and lending, it could be subject to liability, licensure and regulatory approval and may be forced to change its business practices";
- new laws or regulations (such as those that may stem from the proposed Anti-Counterfeiting Trade Agreement (ACTA) and Trans-Pacific Partnership Agreement (TPP), the European Consumer Rights Directive and the proposed revisions to the European Data Protection Directive) and interpretations of existing laws or regulations...;
- regulatory and legal actions imposing obligations on

(2017), *available at* <http://ssrn.com/abstract=2711059>; Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 *THE CONSUMER FIN. L.Q. REP.* 232 (2016), *available at* <http://ssrn.com/abstract=2786186>.

⁵⁵ See generally Gregory E. Maggs, *Regulating Electronic Commerce*, 50 *AM. J. COMP. L.* 665 (2002), *available at* <http://ssrn.com/abstract=958441>; Lawrence J. Trautman & Alvin Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 *CARDOZO L. REV.* (2017), *available at* <http://ssrn.com/abstract=2730983>.

- our businesses or our users...;
- the impact on PayPal or Bill Me Later of regulations enacted pursuant to new laws regulating financial institutions, including the Dodd-Frank Wall Street Reform and Consumer Protection Act in the U.S., or the Dodd-Frank Act;
 - our ability to manage the costs of compliance with existing and new laws and regulations that affect our businesses...;
 - the actions of our competitors, including the introduction of new stores, channels, sites, applications, services, products and functionality, or changes to the provision of services important to our success, including Internet search and access to smartphones through operating systems;
 - the costs and results of litigation or regulatory actions that involve us;
 - technical difficulties or service interruptions involving our websites;
 - disruptions to services provided to us or our users by third parties...;
 - our ability to comply with the requirements of entities whose services are required for our operations, such as payment card networks and banks...;
 - the continued healthy operation of our technology suppliers and other parties with which we have commercial relations;
 - continued consumer acceptance of the Internet and of mobile devices as a medium for commerce and payments in the face of increasing publicity about data privacy issues, including breaches, fraud, spoofing, phishing, viruses, spyware, malware and other dangers...⁵⁶

If our Payments business is found to be subject to or in violation of any laws or regulations, including those governing money transmission, electronic funds transfers, money laundering, terrorist financing, sanctions,

⁵⁶ eBay Form 10-K *supra* note 26 at 13.

consumer protection, banking and lending, it could be subject to liability, licensure and regulatory approval and may be forced to change its business practices.

Our Payments business is subject to various laws and regulations in the U.S. and other countries where it operates, including those governing money transmission, electronic funds transfers, money laundering, terrorist financing, sanctions, consumer protection, banking and lending. The legal and regulatory requirements that apply to our Payments business vary in the markets where we operate. While PayPal has a compliance program focused on compliance with applicable laws and regulations and has significantly increased the resources of that program in the last several years, there can be no assurance that we will not be subject to fines or other enforcement actions in one or more jurisdictions or be required to make changes to our business practices or compliance programs to comply in the future.⁵⁷

Use of Credit Cards

While PayPal currently allows its customers with credit cards to send payments from approximately 190 markets, PayPal only allows customers in 110 of those markets (including the U.S.) to receive payments, in some cases with significant restrictions on the manner in which customers can withdraw funds. These limitations may affect PayPal's ability to grow in these markets. Of the markets whose residents can use the PayPal service, 31 (27 countries plus four French overseas departments) are members of the European Union, or EU. Since 2007, PayPal has provided localized versions of its service to customers in the EU through PayPal (Europe) S.à r.l. et Cie, SCA, a wholly-owned subsidiary of PayPal that is licensed and subject to regulation as a bank in Luxembourg by the Commission de Surveillance du Secteur Financier (CSSF). Accordingly, PayPal (Europe) is subject to significant fines or other enforcement action if it violates the disclosure, reporting, anti-money laundering, capitalization, funds management, corporate governance, information security, sanctions or other requirements imposed on Luxembourg banks. Any fines or other enforcement actions imposed by the Luxembourg regulator could adversely affect PayPal's business. PayPal (Europe) implements its localized services in EU countries through a "passport" notification process through the Luxembourg regulator to regulators in other EU member states pursuant to EU Directives, and has completed the "passport" notification process in all EU member countries. The regulators in these countries could notify PayPal (Europe) of local

⁵⁷ *Id.* at 15.

consumer protection laws that apply to its business, in addition to Luxembourg consumer protection law, and could also seek to persuade the Luxembourg regulator to order PayPal (Europe) to conduct its activities in the local country through a branch office. These or similar actions by these regulators could increase the cost of, or delay, PayPal's plans for expanding its business in EU countries. In addition, national interpretations of regulations implementing the EU Payment Services Directive, which established a new regulatory regime for payment services providers in 2009, may be inconsistent, which could make compliance more costly and operationally difficult to manage.⁵⁸

U.S. State Money Transmission Laws

To date, PayPal has obtained licenses to operate as a money transmitter in 45 U.S. states, the District of Columbia and Puerto Rico. PayPal is also licensed as an escrow agent in one U.S. state. PayPal is applying for money transmitter licenses in two additional states to facilitate its planned offering of payment services at the retail point of sale. The two remaining U.S. states where PayPal has not applied for a license do not currently regulate money transmitters. As a licensed money transmitter, PayPal is subject to restrictions on its investment of customer funds, reporting requirements, bonding requirements, and inspection by state regulatory agencies. If PayPal were found to be in violation of money services laws or regulations, PayPal could be subject to liability and/or additional restrictions, forced to cease doing business with residents of certain states, forced to change its business practices, or required to obtain additional licenses or regulatory approvals that could impose a substantial cost on PayPal. Any change to PayPal's business practices that makes the service less attractive to customers or prohibits its use by residents of a particular jurisdiction could also decrease the velocity of trade on eBay and websites operated by GSI's clients that accept PayPal as a form of payment, which would further harm our business.⁵⁹

⁵⁸ *Id.* See also Paul Benjamin Lowry, Taylor Michael Wells, Greg Daniel Moody, Sean Humphreys & Degan Kettles, *Online Payment Gateways Used to Facilitate E-Commerce Transactions and Improve Risk Management*, 17 COMMUNICATIONS ASSN. INFO. SYS. (CAIS), 1-48, (2006), available at <http://ssrn.com/abstract=879797>.

⁵⁹ eBay Form 10-K *supra* note 26 at 16; See also Kevin V. Tu, *From Bike Messengers to App Stores: Regulating the New Cashless World*, 65 ALA L.R. (2013), available at <http://ssrn.com/abstract=2235937>, Financial Crimes Enforcement Network, United States Department of the Treasury, http://www.fincen.gov/statutes_regs/bsa/ (last visited Aug. 25, 2015), citing Uniform Money Services Act, Prefatory Note, Section A (2004), http://www.uniformlaws.org/shared/docs/money%20services/umsa_final04.pdf (last visited Aug. 25, 2015) (noting that state laws are 'extremely varied'), and Cal. Fin. Code §1800 (2012) (the purpose is to protect the

Our business is subject to online security risks, including security breaches.

[PayPal's (eBay's)] businesses involve the storage and transmission of users' proprietary information, and security breaches could expose [eBay] to a risk of loss or misuse of this information, litigation and potential liability. An increasing number of websites, including several other large Internet companies, have disclosed breaches of their security, some of which have involved sophisticated and highly targeted attacks on portions of their sites. Because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems, change frequently and often are not recognized until launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures. If an actual or perceived breach of our security occurs, public perception of the effectiveness of our security measures could be harmed and we could lose users. A party that is able to circumvent our security measures could misappropriate our or our users' proprietary information, cause interruption in our operations, damage our computers or those of our users, or otherwise damage our reputation and business. Any compromise of our security could result in a violation of applicable privacy and other laws, significant legal and financial exposure, damage to our reputation and a loss of confidence in our security measures, which could harm our business. Data security breaches may also result from non-technical means, for example, actions by a suborned employee...

A significant number of our users authorize us to bill their payment card accounts directly for all transaction fees charged by us. For example, PayPal's users routinely provide payment card and other financial information... We rely on encryption and authentication technology licensed from third parties to provide the security and authentication to effectively secure transmission of confidential information, including customer payment card numbers. Advances in computer capabilities, new discoveries in the field of cryptography or other developments may result in the technology used by us to protect transaction data being breached or compromised. Financial services regulators in various jurisdictions, including the U.S. and the EU, have implemented or are considering proposals to impose new authentication requirements on banks and payment processors intended to reduce online fraud (e.g., two-factor authentication to verify a user's identity), which could impose significant costs on PayPal,

interests of consumers); VA Code Ann. § 6.1-371 (2012) (the statute shall be construed for the purpose of protecting, against financial loss, citizens of Virginia who purchase money orders or control of their funds or credit into the custody of another person for transmission).

Ed 2] *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal* 289

require PayPal to change its business practices, make it more difficult for new customers to join its network and reduce the ease of use of its products, which could harm PayPal's business.

Under payment card rules and our contracts with our card processors, if there is a breach of payment card information that we store, or that is stored by PayPal's direct payment card processing customers, we could be liable to the payment card issuing banks for their cost of issuing new cards and related expenses. In addition, if we fail to follow payment card industry security standards, even if customer information has not been compromised, we could incur significant fines or lose our ability to give customers the option of using payment cards to fund their payments or pay their fees. If we were unable to accept payment cards, our businesses would be seriously damaged.

Our servers are also vulnerable to computer viruses, physical or electronic break-ins and similar disruptions, and we have experienced "denial-of-service" type attacks on our system that have, in certain instances, made all or portions of our websites unavailable for periods of time. For example, in December 2010, PayPal was subject to a series of distributed "denial of service" attacks following PayPal's decision to indefinitely restrict the account used by WikiLeaks due to an alleged violation of PayPal's Acceptable Use Policy. We may need to expend significant resources to protect against security breaches or to address problems caused by breaches. These issues are likely to become more difficult and costly as we expand the number of places where we operate. Security breaches, including any breaches of our security measures or those of parties with which we have commercial relationships (e.g., our clients and third-party service providers) that result in the unauthorized release of users' personal information, could damage our reputation and expose us to a risk of loss or litigation and possible liability. Our insurance policies carry low coverage limits, which may not be adequate to reimburse us for losses caused by security breaches.

Our users, as well as those of other prominent Internet companies, have been and will continue to be targeted by parties using fraudulent "spoof" and "phishing" emails to misappropriate user names, passwords, payment card numbers, or other personal information or to introduce viruses or other malware through "trojan horse" programs to our users' computers. These emails appear to be legitimate emails sent by eBay, PayPal, a GSI client, StubHub or one of our other businesses, or by a user of one of our businesses, but direct recipients to fake websites operated by the sender of

the email or request that the recipient send a password or other confidential information through email or download malware. Despite our efforts to mitigate “spoof” and “phishing” emails through product improvements and user education, “spoof” and “phishing” activities remain a serious problem that may damage our brands, discourage use of our websites and increase our costs.

Changes in regulations or user concerns regarding privacy and protection of user data could adversely affect our business.

We are subject to laws relating to the collection, use, retention, security and transfer of personally identifiable information about our users, especially for financial information and for users located outside of the U.S. As an entity licensed and subject to regulation as a bank in Luxembourg, PayPal (Europe) S.à r.l et Cie, SCA is subject to banking secrecy laws. In many cases, these laws apply not only to third-party transactions, but also to transfers of information between ourselves and our subsidiaries, and between ourselves, our subsidiaries and other parties with which we have commercial relations. In particular, the collection and use of personal information by companies has come under increased regulatory scrutiny. The interpretation and application of user data protection laws are in a state of flux, and may be interpreted and applied inconsistently from country to country.

Regulatory scrutiny of privacy and user data protection is increasing on a global basis, and a number of countries in which we operate are actively evaluating changes to their privacy laws and regulations. The European Union recently proposed new data laws that give customers additional rights and provide additional restrictions and harsher penalties on companies for illegal collection and misuse of personal information, including restrictions on the use of Internet tracking tools called “cookies.” While the European Union directive on cookies has taken effect, the manner in which member states adopt implementing legislation, and whether the European Union deems that legislation sufficient, continues to evolve. To the extent implementing legislation by member states is more restrictive, it could negatively impact the manner in which we use cookies for many of our services, ranging from advertising to anti-fraud, and require us to incur additional costs or change our business practices, which could harm our business. The European Union has also proposed a General Data Protection Regulation that would supersede the European Data Protection Directive. In the U.S., the Federal Trade Commission, or FTC, and the White House have both proposed U.S. privacy frameworks, and in 2012, legislation was

introduced in the U.S. Senate which would have required organizations that suffer a breach of security related to personal information to notify owners of the breached information and, in some instances, notify the Federal Bureau of Investigation or U.S. Secret Service; similar legislation may be introduced and enacted in the future. Other countries in which we operate have recently adopted and implemented privacy and data protection laws and regulations for the first time, or are in the process of doing so. Our current data protection policies and practices may not be consistent with new laws and regulations or evolving interpretations and applications. It is unclear how the application of existing privacy laws and regulations will impact mobile services and technologies, which are evolving rapidly. Complying with these varying national requirements could cause us to incur substantial costs or require us to change our business practices in a manner adverse to our business.

In addition, we have and post on our websites our own privacy policies and practices concerning the collection, use and disclosure of user data. Any failure, or perceived failure, by us to comply with our posted privacy policies or with any regulatory requirements or orders or other federal, state or international privacy or consumer protection-related laws and regulations (or, in the case of our GSI businesses, any such failure or perceived failure on the part of GSI or GSI's clients) could result in proceedings or actions against us by governmental entities or others (e.g., class action privacy litigation), subject us to significant penalties and negative publicity, require us to change our business practices, increase our costs and adversely affect our business. The FTC and state regulatory agencies have become more aggressive in enforcing privacy and data protection laws and regulations. For example, the FTC recently entered into a number of consent decrees with a number of major online companies, including Facebook and Google, to settle allegations of unfair or deceptive privacy practices. The FTC's consent decrees with Facebook and Google require each of those companies to implement a comprehensive privacy program and undergo regular, independent privacy audits for the next 20 years, among other requirements. In December 2012, California's attorney general filed a lawsuit against Delta Air Lines for failing to include a privacy policy in its mobile apps.⁶⁰

⁶⁰ eBay Form 10-K *supra* note 26 at 26. *See also* Christian Biener, Martin Eling & Jan Hendrik Wirfs, *Insurability of Cyber Risk: An Empirical Analysis* (2015). University of St. Gallen, School of Finance Research Paper No. 2015/03, *available at* <http://ssrn.com/abstract=2577286>; Annemarie Bridy, *Internet Payment Blockades* 67 FLA. L. REV. 1523 (2015), *available at* <http://ssrn.com/abstract=2494019>; Kevin Dowd, *New Private Monies: A Bit-Part Player?*, Institute of Economic Affairs Monographs, Hobart Paper 174 (2014), *available at* <http://ssrn.com/abstract=2535299>; Yogesh Malhotra, *Risk, Uncertainty, and Profit for the Cyber Era: Model Risk*

Certain of our businesses, including GSI's interactive marketing services business, utilize "behavioral marketing" (generally, the tracking of a user's online activities) to deliver relevant content to Internet users. The FTC has released a Staff Report with principles to address consumer privacy issues that may arise from behavioral marketing and to encourage industry self-regulation. In March 2012, the FTC issued a final report titled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,"⁶¹ which details the FTC's perspective on best practices for companies that collect and use consumer data to protect the privacy of consumers. Should the FTC pursue enforcement actions related to these business practices, we may have to modify our business practices to conform and incur substantial costs, which could harm our business. In addition, legislators and regulators in various jurisdictions are increasingly focusing on the capture and use of location-based information relating to users of smartphones and other mobile devices, which may result in additional restrictions being placed on the collection and use of such information. Any such regulations or legislation could, if enacted, prohibit the use of certain technologies, including those that track individuals' activities on the Internet or geolocation via mobile devices. Such laws and regulations could restrict our ability to collect and use page viewing data and personal information, which may reduce demand for our services or require changes to our current business models, such as advertising, which could harm our business.

Even technical violations of certain privacy-related laws can result in significant penalties, including statutory damages. The Federal Communications Commission recently amended its regulations under the Telephone Consumer Protection Act (TCPA), effective in July 2012, which could increase our exposure to liability for certain types of telephonic communication with customers, including but not limited to text messages to mobile phones. Under the TCPA, plaintiffs may seek actual monetary loss or statutory damages of \$500 per violation, whichever is greater, and courts may treble the damage award for willful or knowing violations. Two putative class-action lawsuits have been filed containing allegations that our businesses violated the TCPA. *Roberts v. PayPal* (filed in the U.S. District

Management of Cyber Insurance Models Using Quantitative Finance and Advanced Analytics (2015), available at <http://ssrn.com/abstract=2553547>; Philip Rawlings, *Cyber Risk: Insuring the Digital Age*, 128 BRIT. INS. L. ASS'N J. (2015), available at <http://ssrn.com/abstract=2551421>.

⁶¹ FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326_privacyreport.pdf. (last visited Sept. 4, 2016).

Court for the Northern District of California in February 2012) contains allegations that commercial advertisements for PayPal products and services were sent via text message to mobile phones without prior consent. *Murray v. Bill Me Later* (filed in the U.S. District Court for the Northern District of Illinois in June 2012) contains allegations that Bill Me Later made calls featuring artificial or prerecorded voices without prior consent. These lawsuits seek damages (including statutory damages) and injunctive relief, among other remedies. Given the enormous number of communications we send to our users, a determination that there have been violations of laws relating to PayPal's or Bill Me Later's practices (or those of any of our other companies) under the TCPA or other communications-based statutes could expose us to significant damage awards that could, individually or in the aggregate, materially harm our business.

Data collection, privacy and security have become the subject of increasing public concern. If Internet and mobile users were to reduce their use of our websites, mobile platforms, products and services as a result, our business could be harmed. As noted above, we are also subject to the possibility of security breaches, which themselves may result in a violation of these laws.⁶²

New and existing regulations could harm our business.

We are subject to the same foreign and domestic laws as other companies conducting business on and off the Internet. It is not always clear how existing laws governing issues such as property ownership, copyrights, trademarks and other intellectual property issues, parallel imports and distribution controls, consumer protection, taxation, libel and defamation, obscenity and personal privacy apply to online businesses such as ours. Many of these laws were adopted prior to the advent of the Internet and related technologies and, as a result, do not contemplate or address the unique issues of the Internet and related technologies. Those laws that do reference the Internet, such as the U.S. Digital Millennium Copyright Act, the U.S. "CAN-SPAM" Act and the European Union's Distance Selling Directive (which will be superseded by the new Consumer Rights Directive, which the member states are in the process of implementing) and Electronic Commerce Directive are being interpreted by the courts, but their applicability and scope remain uncertain. As our activities, the types of goods and services listed on our websites, the products and services we offer (including through acquisitions such as Bill Me Later and StubHub)

⁶² eBay Form 10-K *supra* note 26 at 28.

and our geographical scope continue to expand, regulatory agencies or courts may claim or hold that we or our users are subject to additional requirements (including licensure) or prohibited from conducting our business in their jurisdiction, either generally or with respect to certain actions (e.g., the sale of real estate, event tickets, cultural goods, boats and automobiles, or the application of distance selling laws). Recent financial and political events may increase the level of regulatory scrutiny on large companies in general, and financial services companies in particular, and regulatory agencies may view matters or interpret laws and regulations differently than they have in the past and in a manner adverse to our businesses.

Our success and increased visibility has driven some existing businesses that perceive our business models to be a threat to their businesses to raise concerns about our business models to policymakers and regulators. These established businesses and their trade association groups employ significant resources in their efforts to shape the legal and regulatory regimes in countries where we have significant operations. They may employ these resources in an effort to change the legal and regulatory regimes in ways intended to reduce the effectiveness of our businesses and the ability of users to use our products and services. In particular, these established businesses have raised concerns relating to pricing, parallel imports, professional seller obligations, selective distribution networks, stolen goods, copyrights, trademarks and other intellectual property rights and the liability of the provider of an Internet marketplace for the conduct of its users related to those and other issues. Any changes to the legal or regulatory regimes in a manner that would increase our liability for third-party listings could negatively impact our business.⁶³

Following the global financial crisis, U.S. federal lawmakers enacted the Dodd-Frank Act overhauling the federal government's oversight of consumer financial products and systemic risk in the U.S. financial system. Although the full effect of the new legislation will be dependent on regulations to be adopted by a number of different agencies (including the recently created Consumer Financial Protection Bureau), we expect the general effect of the financial reform law will be to require PayPal and Bill Me Later to make additional disclosures to their users and to impose new restrictions on certain of their activities. For example, in January 2012, the Consumer Financial Protection Bureau finalized new regulations, required by the Dodd-Frank Act that will require PayPal, starting in 2013, to provide

⁶³ *Id.* at 29.

additional disclosures, error resolution rights and cancellation rights to U.S. consumers who make international remittance payments, which could increase our costs of processing international payments. These and other new obligations will impose new compliance requirements and obligations on us that could increase our costs, may result in increased litigation and the need to make expensive product changes and may otherwise adversely impact our business.

In addition, we also expect that the continued implementation of the Dodd-Frank Act will adversely impact some significant traditional revenue streams for banks. For example, in June 2011, the Federal Reserve Board issued a final rule capping debit card interchange fees. As a result of this and other regulations implementing the financial reform law, banks may need to revise their business models to remain profitable, which may lead them to charge more for services which were previously provided for free or at lower cost. Any resulting increases in service fees required for PayPal to process transactions (e.g., service fees for automated clearing house transactions) would increase our costs and could adversely affect our business.⁶⁴

Online and Mobile Growth Dependence

We depend on the continued growth of online and mobile commerce.

The business of selling goods over the Internet and mobile networks, particularly through online trading, is dynamic and relatively new. Concerns about fraud, privacy and other problems may discourage additional consumers from adopting the Internet or mobile devices as modes of

⁶⁴ *Id.* at 30; See also Stephen M. Bainbridge, *Dodd-Frank: Quack Federal Corporate Governance Round II*, UCLA Sch. of Law, Law-Econ. Research Paper No. 10-12 (2010), available at <http://ssrn.com/abstract=1673575>; Lissa L. Broome, *The Dodd-Frank Act: Tarp Bailout Backlash and Too Big to Fail*, 15 North Carolina Banking Institute, 101 (2011); UNC Legal Stud. Research Paper No. 1794271, available at <http://ssrn.com/abstract=1794271>; John C. Coffee, *The Political Economy of Dodd-Frank: Why Financial Reform Tends to be Frustrated and Systemic Risk Perpetuated*, CORNELL L.R. (2012), available at <http://ssrn.com/abstract=1982128>; Roberta Romano, *Regulating in the Dark*, Yale Law & Econ. Research Paper No. 442 (2012), available at <http://ssrn.com/abstract=1974148>; David A. Skeel, *The New Financial Deal: Understanding the Dodd-Frank Act and its (Unintended) Consequences*, in *THE NEW FINANCIAL DEAL: UNDERSTANDING THE DODD-FRANK ACT AND ITS (UNINTENDED) CONSEQUENCES*, Wiley, 2010), available at <http://ssrn.com/abstract=1690979>; Andrew Verstein & Roberta Romano, *Assessing Dodd-Frank* Yale Law & Econ. Research Paper No. 434 (2011) available at <http://ssrn.com/abstract=1884290>; Arthur E. Wilmarth, *The Dodd-Frank Act: A Flawed and Inadequate Response to the Too-Big-To-Fail Problem*, 89 OR. L. REV. 951 (2011), available at <http://ssrn.com/abstract=1719126>.

commerce, or may prompt consumers to offline channels. In countries such as the U.S., Germany, Korea and the U.K., where our services and online commerce generally have been available for some time and the level of market penetration of our services is high, acquiring new users for our services may be more difficult and costly than it has been in the past. Moreover, the growth rates of Internet users are slowing in many countries where we have a significant presence. In order to expand our user base, we must appeal to and acquire consumers who historically have used traditional means of commerce to purchase goods and may prefer Internet analogues to such traditional retail means, such as the retailer's own website, to our offerings. If these consumers prove to be less active than our earlier users due to lower levels of willingness to use the Internet or mobile devices for commerce for any reason, including lack of access to high-speed communications equipment, congestion of traffic on the Internet, Internet or mobile network outages or delays, disruptions or other damage to users' computers or mobile devices, and we are unable to gain efficiencies in our operating costs, including our cost of acquiring new users, our business could be adversely impacted.

Reliance on Internet Access

Our businesses depend on continued and unimpeded access to the Internet, as well as access to mobile networks. Internet service providers and mobile network operators may be able to block, degrade, or charge us or our users additional fees for our offerings, which could harm our business.

Our customers rely on access to the Internet or mobile networks to use our products and services. In many cases, that access is provided by companies that compete with at least some of our offerings, including incumbent telephone companies, cable companies, mobile communications companies and large Internet service providers. Some of these providers have stated that they may take measures that could degrade, disrupt, or increase the cost of customers' use of our offerings by restricting or prohibiting the use of their infrastructure to support or facilitate our offerings, or by charging increased fees to us or our users to provide our offerings. Mobile network operators or operating system providers could block or place onerous restrictions on our ability to offer our mobile applications in their mobile application stores. Internet service providers or mobile network operators could attempt to charge us each time our customers use our offerings. Worldwide, a number of companies have announced plans to take such actions or are selling products designed to facilitate such actions. The United States Federal Communications

Commission enacted rules in December 2010 (*Preserving the Open Internet Broadband Industry Practices (FCC-10-201)*) establishing baseline restrictions that would regulate the ability of Internet access companies to interfere with Internet traffic transported over wired and wireless networks. A decision from the D.C. Circuit Court of Appeals is expected in early 2013. Pending greater regulatory and judicial clarity, any interference with our offerings or higher charges for access to our offerings, whether paid by us or by our customers, could cause us to lose existing customers, impair our ability to attract new customers and harm our revenue and growth.

Our business depends on the development and maintenance of the Internet infrastructure.

The success of our services will depend largely on the development and maintenance of the Internet infrastructure. This includes maintenance of a reliable network backbone with the necessary speed, data capacity, and security, as well as timely development of complementary products, for providing reliable Internet access and services. The Internet has experienced, and is likely to continue to experience, significant growth in the numbers of users and amount of traffic. The Internet infrastructure may be unable to support such demands. In addition, increasing numbers of users, increasing bandwidth requirements, or problems caused by “viruses,” “worms,” malware and similar programs may harm the performance of the Internet. The backbone computers of the Internet have been the targets of such programs. From time to time, the Internet has experienced, and is likely to continue to experience, a variety of outages and other delays as a result of damage to portions of its infrastructure. Any such outages and delays could reduce the level of Internet usage generally as well as the level of usage of our services, which could adversely impact our business.⁶⁵

VII. INTERNATIONAL EXPANSION

Like many U.S.-based entities, over half of PayPal’s total revenues are from non-U.S.-sources (for the sixth consecutive quarter), “PayPal revenues for Q1 2013 were \$1.5 billion [US], growing 20% year over year on an FX neutral basis, [while]... international business generated \$795 million in revenue in Q1

⁶⁵ *Id.* at 49. See also Elizabeth Eraker, Colin Hector, Chris Jay Hoofnagle, *Mobile Payments: The Challenge of Protecting Consumers and Innovation*, 10 PRIVACY & SEC. L. RPT. 212 (2011), available at <http://ssrn.com/abstract=2428175>; Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015), available at <http://ssrn.com/abstract=2485550>.

2013, and international revenue grew at a rate of 19% year over year.”⁶⁶ PayPal’s worldwide expansion brings increased cost of doing business by virtue of increased internal control challenges and because of being subjected to numerous and often conflicting laws and regulations including: conflicting local values,⁶⁷ data privacy and filtering rules;⁶⁸ disclosure and internal control rules;⁶⁹ anti-corruption laws such as the Foreign Corrupt Practices Act (FCPA) and U.K. Bribery Act 2010;⁷⁰ intellectual property considerations,⁷¹ and business practices or laws favoring local competitors.⁷² Professor Tabrez Ahmad observes

⁶⁶ PayPal, *supra* note 36.

⁶⁷ See generally Christoph Engel & Kenneth H. Keller, *Global Networks and Local Values*, available at <http://ssrn.com/abstract=307039>; Olufunmilayo Arewa, *Measuring and Representing the Knowledge Economy: Accounting for Economic Reality Under the Intangibles Paradigm*, 54 BUFF. L. REV., (2006); Case Legal Stud. Research Paper No. 04-14, available at: <http://ssrn.com/abstract=589205>.

⁶⁸ See generally Derek E. Bambauer, *Filtering in Oz: Australia’s Foray into Internet Censorship* (December 22, 2008), Brooklyn Law Sch., Legal Stud. Paper No. 125, available at: <http://ssrn.com/abstract=1319466>; Derek E. Bambauer, Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, Nart Villeneuve & Jonathan Zittrain, *Internet Filtering in China in 2004-2005: A Country Study*, Berkman Center for Internet & Society at Harvard Law Sch. Research Publication No. 2005-10 (April 15, 2005), available at <http://ssrn.com/abstract=706681>; Derek E. Bambauer, *Orwell’s Armchair*, 79 U. CHI. L. REV. 863 (2012), available at: <http://ssrn.com/abstract=1926415>; Derek E. Bambauer, *Cybersieves*, 59 DUKE L. J. (2009), available at: <http://ssrn.com/abstract=1143582>; Derek E. Bambauer, *Censorship V3.1*, 18 IEEE INTERNET COMPUTING 26 (May/June 2013), available at <http://ssrn.com/abstract=2144004>; Christopher Kuner, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 1)*, 18 INT’L J. L. & INFO. TECH., 176 (2010), available at: <http://ssrn.com/abstract=1496847>; Christopher Kuner, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2)*, 18 INT’L J.L.& INFO. TECH., 227 (2010), available at: <http://ssrn.com/abstract=1689495>; Mary C. Rundle & Ben Laurie, *Identity Management as a Cybersecurity Case Study* (2005), Berkman Center Research Publication No. 2006-01, available at <http://ssrn.com/abstract=881107>;

⁶⁹ See generally Paola Musile Tanzi, Adalberto Alberici, Giampaolo Gabbi, Manuela Gallo, Loris Nadotti, Raoul Pisani, Maurizio Poli, Daniele Angelo Previati, Paola Schwizer, Valeria Stefanelli & Renata Trinca Colonel, *The Evolution of Compliance Function and Compliance Risk in Investment Services* (June 2009), available at <http://ssrn.com/abstract=1446759>; Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COMM. L.J. 205 (2013), available at <http://www.ssrn.com/abstract=2137747>.

⁷⁰ See Lawrence J. Trautman & Kara Altenbaumer-Price, *The Foreign Corrupt Practices Act: Minefield for Directors*, 6 VA. L. & BUS. REV. 145 (2011), available at <http://www.ssrn.com/abstract=1930190>; Lawrence J. Trautman & Kara Altenbaumer-Price, K., *Lawyers, Guns and Money – The Bribery Problem and U.K. Bribery Act*, 47 INT’L LAW. 481 (2013), available at <http://www.ssrn.com/abstract=2276738>.

⁷¹ See generally Frederick M. Abbott, *Intellectual Property, International Protection*, V MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 228 (Rüdiger Wolfrum ed.) (Oxford 2012), available at <http://ssrn.com/abstract=2080214>; Frederick M. Abbott, *Intellectual Property Rights in World Trade*, in RESEARCH HANDBOOK IN INTERNATIONAL ECONOMIC LAW, 444, A. Guzman & A. Sykes, eds., Edward Elgar, (2007), available at <http://ssrn.com/abstract=1984855>; Olufunmilayo Arewa, *Piracy, Biopiracy and Borrowing*:

...That the internet is a worldwide application. It involves international protocols and conventions as well as state and national legislation...

The factors that are driving Internet applications include the expanding global communication networks, the expansion of global online markets, and the emerging of business models that provide access to the global market. Business strategies have evolved from the bricks and mortar retail establishments, and catalogue outlets into electronic business transactions that run the full cycle from procurement of raw materials, to processing and distribution of manufactured goods, to order fulfillment systems and international payment processes via electronic funds transfer systems.

In addition to the international sale of goods, there is a blossoming of electronic services that were previously only available through hard line links to service providers. Internet retailing, banking, and data exchange now flow over computer grids and satellite systems. Deals are closed not with a handshake, but with an exchange of private keys.

Cyberspace is the complete value chain that links suppliers, producers, retailers, and customers. Companies that do not plan to enter the e-Commerce arena themselves, still have to deal with clients and customers whose only presence will be in the form of full-service electronic storefronts. These companies will have to adjust their strategic plan to include electronic media in their businesses. Understanding the novel legal issues that arise in relation to, the Internet, electronic commerce and online services, as well as the laws and jurisdictional matters that apply to e-commerce applications, will be the instrument of success in positioning a business in the electronic marketplace.⁷³

Culture, Cultural Heritage and the Globalization of Intellectual Property, Case Legal Stud. Research Paper No. 04-19 (2006), available at <http://ssrn.com/abstract=596921>; Derek Slater, Urs Gasser, Meg Smith, Derek E. Bambauer & John G. Palfrey, *Content and Control: Assessing the Impact of Policy Choices on Potential Online Business Models in the Music and Film Industries*, Berkman Publication Series Paper No. 2005-01, available at: <http://ssrn.com/abstract=654602>.

⁷² See Generally Selby & Manning, *supra* note 15; Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TUL. L. REV. (1998), available at <http://ssrn.com/abstract=127308>.

⁷³ Tabrez Ahmad, *Information & Communication Technology Law* (December 7, 2011), available at <http://ssrn.com/abstract=1969493>.

Anti-Corruption

Corruption in any of its various forms is a problem for any business. Previously, many have documented numerous examples of how the potential for significant exposure to international corruption and anti-bribery laws increases with expanding U.S. business operations around the globe.⁷⁴ eBay has adopted a “strict policy of doing business based on the merits of our services, not based on any form of bribery, or any other corrupt or unethical business practice. Our Code of Business Conduct outlines our policies and principles on bribery and extortion in countries around the world.”⁷⁵ In addition

The United States and countries around the world strictly prohibit the bribery of government officials, and we abide by these laws and regulations. We educate our employees to ensure that they do not intentionally or inadvertently make any unlawful payment, kickback, or gift to any US or foreign government official or candidate for office in order to get or keep business...

We operate a 24-hour help line that employees can call or email to make anonymous reports of violations, or ask questions about our anti-bribery and AML policies, as well as Code of Business Conduct. Additionally, our Business Ethic Officers are able to provide in-person assistance and guidance to employees who wish to raise concerns.

We treat all reports as confidential to the extent permitted by laws, and have a strict no-retaliation policy for those who reported misconduct in good faith.

⁷⁴ See generally Norman D. Bishara, *Governance and Corruption Constraints in the Middle-East: Overcoming the Business Ethics Glass Ceiling*, 48 AM. BUS. L.J. 227 (2011); Trautman & Altenbaumer-Price, *supra* note 51; ; Mike Koehler, *A Foreign Corrupt Practices Act Narrative*, 22 MICH. ST. INT’L L. REV. 961 (2014), available at <http://ssrn.com/abstract=2428555>; Mike Koehler, *Ten Seldom Discussed Foreign Corrupt Practices Act Facts that You Need to Know*, 10 BLOOMBERG BNA WHITE COLLAR CRIME REPORT 347 (May 1, 2015), available at <http://ssrn.com/abstract=2601840>; Virginia G. Maurer & Ralph E. Maurer, *Uncharted Boundaries of the U.S. Foreign Corrupt Practices Act*, 20 J. FIN. CRIME 355 (2013); Gideon Mark, *Private FCPA Enforcement*, 49 AM. BUS. L.J. 419 (2012); Philip M. Nichols, *The Business Case for Complying with Bribery Laws*, 49 AM. BUS. L.J. 325 (2012); Peter R. Reilly, *Incentivizing Corporate America to Eradicate Transnational Bribery Worldwide: Federal Transparency and Voluntary Disclosure Under the Foreign Corrupt Practices Act*, 67 FLA. L. REV. 1683 (2015), available at <http://ssrn.com/abstract=2585789>; Lawrence J. Trautman & Kara Altenbaumer-Price, *The Foreign Corrupt Practices Act: Minefield for Directors*, 6 VA L. & BUS. REV. 145 (2011), available at <http://www.ssrn.com/abstract=1930190>; Lawrence J. Trautman & Kara Altenbaumer-Price, *Foreign Corrupt Practices Act: An Update on Enforcement and SEC and DOJ Guidance*, 41 SEC. REG. L.J. 241 (2013), available at <http://ssrn.com/abstract=2293382>;

⁷⁵ See eBay Global Compact Report 7 (2012), available at http://legacy.ebayinc.com/assets/pdf/fact_sheet/eBay_UNGCR_2012_FINAL.pdf.

As of 2012, no eBay employees were cited for infraction of our anti-bribery policies. We hired an Anti-Corruption Officer based in Asia who is focused on building out a robust compliance program, which ensures that eBay complies with all applicable anti-corruption laws around the world.⁷⁶

Here is the disclosure regarding international expansion from PayPal:

Localization (is Expensive)

As we expand and localize our international activities, we may become obligated to comply with the laws of the countries or markets in which we operate. In addition, because our services are accessible worldwide and we facilitate sales of goods and provide services to users worldwide, one or more jurisdictions may claim that we or our users are required to comply with their laws based on the location of our servers or one or more of our users, or the location of the product or service being sold or provided in an ecommerce transaction. For example, in the Louis Vuitton Malletier litigation, we were found liable in France, under French law, for transactions on some of our websites worldwide that did not involve French buyers or sellers... Laws regulating Internet and ecommerce companies outside of the U.S. are generally be less favorable than those in the U.S., giving greater rights to consumers, content owners, competitors, users and other third parties. Compliance may be more costly or may require us to change our business practices or restrict our service offerings, and the imposition of any regulations on us or our users may harm our business. In addition, we may be subject to multiple overlapping legal or regulatory regimes that impose conflicting requirements on us (e.g., in cross-border trade). Our alleged failure to comply with foreign laws could subject us to penalties ranging from criminal prosecution to significant fines to bans on our services, in addition to the significant costs we may incur in defending against such actions.⁷⁷

PayPal On International Risk

As we continue to expand our businesses internationally, including through acquisitions and joint ventures, we are increasingly subject to risks of doing business internationally, including the following:

⁷⁶ *Id.*

⁷⁷ eBay Form 10-K *supra* note 26 at 30; *See also* Michael L. Rustad, *Circles of E-Commerce Trust: Old America v. New Europe*, 16 MICH. ST. J. INT'L L. 183 (2007), available at <http://ssrn.com/abstract=1023659> (observing there is a chasm between U.S. and European consumer protection rules in cyberspace).

- strong local competitors;
- regulatory requirements, including regulation of Internet and mobile services, auctioneering, professional selling, distance selling, privacy and data protection, banking and money transmitting, that may limit or prevent the offering of our services in some jurisdictions, prevent enforceable agreements between sellers and buyers, prohibit the listing of certain categories of goods, require product changes, require special licensure, subject us to various taxes, penalties or audits, or limit the transfer of information between us and our affiliate;
- customs and duties, including the possibility of significant delays at the border due to customs inspections and the possibility that our services may be viewed as facilitating customs fraud by governmental authorities;
- greater liability or legal uncertainty... including uncertainty as a result of unique local laws, conflicting court decisions and lack of clear precedent or applicable law...;
- potentially higher incidence of fraud and corruption and higher credit and transaction loss risks;
- cultural ambivalence towards, or non-acceptance of, trading or payments over the Internet or through mobile devices;
- laws and business practices that favor local competitors or prohibit or limit foreign ownership of certain businesses;
- difficulties in integrating with local payment providers, including banks, credit and debit card networks and electronic fund transfer systems...;
- higher Internet service provider or mobile network operator costs;
- differing intellectual property laws;
- different and more stringent consumer protection, data protection, privacy and other laws...;
- expenses associated with localizing our products and services, including offering customers the ability to transact business in the local currency and adapting our products and services to local preferences (e.g., payment methods) with which we may have limited or

- no experience;
- foreign exchange rate fluctuations;
- our ability to repatriate funds from abroad without adverse tax consequences;
- the possibility that foreign governments may impose currency controls or other restrictions on the repatriation of funds...; and
- challenges associated with maintaining relationships with local law enforcement and related agencies.

Compliance with complex foreign and U.S. laws and regulations that apply to our international operations increases our cost of doing business. These numerous and sometimes conflicting laws and regulations include internal control and disclosure rules, data privacy and filtering requirements, anti-corruption laws, such as the Foreign Corrupt Practices Act and U.K. Bribery Act, and other local laws prohibiting corrupt payments to governmental officials, and antitrust and competition regulations, among others. Violations of these laws and regulations could result in fines and penalties, criminal sanctions against us, our officers, or our employees, prohibitions on the conduct of our business and on our ability to offer our products and services in one or more countries, and could also materially affect our brands, our international expansion efforts, our ability to attract and retain employees, our business, and our operating results. Although we have implemented policies and procedures designed to ensure compliance with these laws and regulations, there can be no assurance that our employees, contractors, or agents will not violate our policies.⁷⁸

⁷⁸ eBay Form 10-K *supra* note 26 at 36, *See also* Noel Cox, *The Extraterritorial Enforcement of Consumer Legislation and the Challenge of the Internet*, 8 EDINBURGH L. REV. 60(2004), available at <http://ssrn.com/abstract=584862> (advocating that electronic commerce requires a balanced approach to co-regulation); Nikhil Joseph & Benjamin D. Mazzotta, *Citrus: India's Answer to Paypal?*, IBGC Working Paper 14-05 (2014), available at <http://ssrn.com/abstract=2095253>; Eliza Karolina Mik, *'Updating' the Electronic Transactions Act? – Australia's Accession to the UN Convention on the Use of Electronic Communications in International Contracts 2005*, 26 J. CONTRACT L., available at <http://ssrn.com/abstract=2046858> (discussing the Australian Government's proposal to accede to the United Nations Convention on the Use of Electronic Communications in International Contracts as well as certain amendments to the Existing Australian electronic transactions legislation); Lawrence J. Trautman & Kara Altenbaumer-Price, *The Foreign Corrupt Practices Act: Minefield for Directors*, 6 VA. L. & BUS. REV. 145 (2011), available at <http://www.ssrn.com/abstract=1930190>; Jonathan Whitaker, Nigel P. Melville, Robert K. Plice, & Jason Dedrick, *Internet Business Practices Across the Globe: Lessons from Emerging Economies*, Ross Sch. of Bus. Paper No. 1113 (2008), available at

China

In China, PayPal is affiliated with Shanghai Wangfuyi Information Technology Ltd., which is licensed as an Internet Content Provider and operates a payments service only for Chinese customers and only for transactions denominated in Chinese currency. The People's Bank of China (PBOC) has enacted regulations to establish a new type of license, called a Payment Clearing Organization (PCO) license, which will be required for non-bank payment services. The PBOC regulations leave unclear whether a foreign-owned company such as PayPal can control or invest in a Payment Clearing Organization, and whether Wangfuyi or PayPal's wholly-owned subsidiary in China would be eligible to obtain a PCO license. Nonetheless, PayPal applied for such a license.⁷⁹

VIII. AML, COUNTER-TERRORIST LAWS, & POTENTIALLY ILLEGAL ACTIVITY

As a money transmitter, PayPal states that they have a firm commitment to “actively deterring and detecting money laundering (AML) and terrorist financing activities. Using a sophisticated system of controls, we aggressively work to report and identify any abnormalities in the transaction system that could be indicators of corrupt activity, coordinating with law enforcement and regulators around the world in this effort.”⁸⁰

PayPal's approach requires that they be proactive in enhancing our current policies to meet regulatory expectations as new geographies, products and services, monitoring authorities or jurisdictional requirements are introduced or developed... In 2012, we updated our mandatory AML training, adding an online compliance component, and hired compliance

<http://ssrn.com/abstract=1017995>; (contending that Firms in emerging economies are rapidly becoming formidable competitors to long-established industry leaders from developed economies).

⁷⁹ eBay Form 10-K *supra* note 26 at 16. See also Frederick M. Abbott, *China in the WTO 2006: 'Law and its Limitations' in the Context of TRIPS*, in *WTO LAW AND DEVELOPING COUNTRIES*, 59, G. Bermann, P. Mavroidis, eds., CAMBRIDGE UNIV. PRESS, (2007), available at <http://ssrn.com/abstract=1919488>; Lawrence J. Trautman, *American Entrepreneur in China: Potholes on the Silk Road to Prosperity*, 12 *WAKE FOREST J. BUS. & INT'L PROP. L.* 427 (2012), available at <http://www.ssrn.com/abstract=1995076>; Trautman & Altenbaumer-Price, *supra* note 55.

⁸⁰ eBay Global Compact Report 7 (2012) available at http://legacy.ebayinc.com/assets/pdf/fact_sheet/eBay_UNGCR_2012_FINAL.pdf. See also Lawrence J. Trautman, *Following the Money: Lessons from the "Panama Papers," Part 1: Tip of the Iceberg* (forthcoming) (discussing AML, payments for bribery, corruption, and terrorism finance), available at <http://ssrn.com/abstract=2783503>.

training managers focusing on our high risk regions. This year, eBay extended our online AML training to contractors, employees, and vendors.⁸¹

AML and Counter-terrorist Laws

PayPal is also subject to various anti-money laundering and counter-terrorist financing laws and regulations around the world that prohibit, among other things, its involvement in transferring the proceeds of criminal activities. PayPal is focused on compliance with these laws and regulations and has programs designed to comply with new and existing legal and regulatory requirements. However, any errors, failures or delays in complying with federal, state or foreign anti-money laundering and counter-terrorist financing laws could result in significant criminal and civil lawsuits, penalties and forfeiture of significant assets or other enforcement actions. In the U.S., PayPal is subject to regulations that require it to report, within required timeframes, suspicious activities involving transactions of \$2,000 or more, and may be required to obtain and keep more detailed records on the senders and recipients in certain transfers of \$3,000 or more. New regulations on prepaid access programs which took full effect in March 2012 require PayPal to take additional steps to verify the identity of customers who pre-fund a PayPal balance. U.S. regulators have increased scrutiny of compliance with these obligations. Existing and new regulations may require PayPal to revise further its compliance program, including the procedures it uses to verify the identity of its customers and to monitor international and domestic transactions.⁸²

Focus on Potentially Illegal Activity

PayPal's payment system is also susceptible to potentially illegal or improper uses, including illegal online gambling, fraudulent sales of goods or services, illicit sales of prescription medications or controlled substances, piracy of software, movies, music and other copyrighted or trademarked goods, money laundering, terrorist financing, bank fraud, child pornography trafficking, prohibited sales of alcoholic beverages or tobacco products, online securities fraud and encouraging, promoting, facilitating or instructing others to engage in illegal activities. There has been an increased focus by rights owners and U.S. government officials on the role that payments systems play in the sale of, and payment for, pirated digital goods

⁸¹ *Id.*

⁸² eBay Form 10-K *supra* note 26 at 17; Miriam A. Goldby, *Anti-Money Laundering Reporting Requirements Imposed by English Law: Measuring Effectiveness and Gauging the Need for Reform*, J. BUS. L., (forthcoming), available at <http://ssrn.com/abstract=2012448>.

on the Internet. Recent changes in law have increased the penalties for intermediaries providing payment services for certain illegal activities and additional payments-related proposals are under active consideration by government policymakers. Despite measures PayPal has taken to detect and lessen the risk of this kind of conduct, illegal activities could still be funded using PayPal. Any resulting claims, liabilities or loss of transaction volume could damage our reputation and harm our business.⁸³

PayPal's highly automated and liquid payment service makes PayPal an attractive target for fraud. In configuring its service, PayPal continually strives to maintain the right balance of appropriate measures to promote both convenience and security for customers. Identity thieves and those committing fraud using stolen payment card or bank account numbers can potentially steal large amounts of money from businesses such as PayPal. We believe that several of PayPal's current and former competitors in the electronic payments business have gone out of business or significantly restricted their businesses largely due to losses from this type of fraud. While PayPal uses advanced anti-fraud technologies, we expect that technically knowledgeable criminals will continue to attempt to circumvent PayPal's anti-fraud systems using increasingly sophisticated methods. From time to time, such fraudsters may discover and exploit vulnerabilities that may not immediately be identified and remediated, which may in turn result in one-time increases in fraud and associated transaction losses, which may be substantial. In addition, because users frequently use the same passwords for different sites, a data breach of a third party site can result in a spike in eBay and/or PayPal transaction losses. PayPal's service could also be subject to employee fraud or other internal security breaches, and PayPal may be required to reimburse customers for any funds stolen as a result of such breaches. Merchants could also request reimbursement, or stop using PayPal, if they are affected by buyer fraud or other types of fraud...⁸⁴

IX. CONCLUSION

The Internet, e-commerce, new technologies, and mobile platforms are having a major impact on those engaged in e-commerce and electronic payment systems. Early recognition of relevant risks may prove helpful in avoiding increases in operating costs and reduce the risks of falling victim to threats

⁸³ eBay Form 10-K *supra* note 26 at 22; *See also* Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014), available at <http://www.ssrn.com/abstract=2393537>, (discusses illegal or improper use of the Internet and virtual payment systems).

⁸⁴ *Id.* at 24.

Ed 2] *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal* 307

involving the very survival of the enterprise. An examination of financial and regulatory disclosures by eBay (parent of PayPal), as filed with the U.S. Securities and Exchange Commission, is helpful to the understanding of risks faced by most participants in the e-commerce and electronic payment systems arena.