PayPal Holdings, Inc.
Form 10-K
February 07, 2019

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

ý ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended December 31, 2018.
OR
o TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the Transition Period from to .
Commission file number 001-36859

PayPal Holdings, Inc.
(Exact Name of Registrant as Specified in Its Charter)

Delaware	47-2989869
(State or Other Jurisdiction of Incorporation or Organization)	(I.R.S. Employer Identification No.)
2211 North First Street San Jose, California	95131
(Address of Principal Executive Offices)	(Zip Code)

(408) 967-1000
(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Name of each exchange on which registered
Common Stock, $0.0001 par value per share	The NASDAQ Stock Market LLC

Securities registered pursuant to Section 12(g) of the Securities Exchange Act of 1934:
None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes [x] No [ ]

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Exchange Act. Yes [ ] No [x]

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the preceding 12 months (or for such shorter period that the registrant was required to file such

reports), and (2) has been subject to such filing requirements for the past 90 days. Yes [x] No [ ]

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes [x] No [ ]

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§ 229.405 of this chapter) is not contained herein, and will not be contained, to the best of the registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. [x]

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” “smaller reporting company,” and “emerging growth company” in Rule 12b-2 of the Exchange Act. :

Large accelerated filer	ý	Accelerated filer	o
Non-accelerated filer	o	Smaller reporting company	o
		Emerging growth company	o

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. o

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes [ ] No [x]

As of June 30, 2018, the aggregate market value of the registrant's common stock held by non-affiliates of the registrant was approximately $98.5 billion based on the closing sale price as reported on the NASDAQ Global Select Market.

As of January 31, 2019, there were 1,173,209,367 shares of common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant’s definitive proxy statement for its 2019 Annual Meeting of Stockholders are incorporated herein by reference in Part III of this Annual Report on Form 10-K to the extent stated herein. Such proxy statement will be filed with the Securities and Exchange Commission within 120 days of the registrant’s fiscal year ended December 31, 2018.

Table of Contents

TABLE OF CONTENTS

		Page
Part I		
Item 1.	Business	4
Item 1A.	Risk Factors	11
Item 1B.	Unresolved Staff Comments	36
Item 2.	Properties	36
Item 3.	Legal Proceedings	36
Item 4.	Mine Safety Disclosures	36
Part II		
Item 5.	Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities	37
Item 6.	Selected Financial Data	38
Item 7.	Management's Discussion and Analysis of Financial Condition and Results of Operations	39
Item 7A.	Quantitative and Qualitative Disclosures About Market Risk	62
Item 8.	Financial Statements and Supplementary Data	63
Item 9.	Changes in and Disagreements With Accountants on Accounting and Financial Disclosure	63
Item 9A.	Controls and Procedures	64
Item 9B.	Other Information	64
Part III		
Item 10.	Directors, Executive Officers and Corporate Governance	64
Item 11.	Executive Compensation	64
Item 12.	Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters	64
Item 13.	Certain Relationships and Related Transactions, and Director Independence	64
Item 14.	Principal Accounting Fees and Services	65
Part IV		
Item 15.	Exhibits, Financial Statement Schedules	65
Item 16.	Form 10-K Summary	122

Presentation of Information

On July 17, 2015, PayPal Holdings, Inc. (“PayPal Holdings”) became an independent publicly traded company through the pro rata distribution by eBay (defined below) of 100% of the outstanding common stock of PayPal Holdings to eBay’s stockholders (which we refer to as the “separation” or the “distribution”). For additional information, see “Business—Separation from eBay Inc.” To accomplish this separation, in January 2015, eBay incorporated PayPal Holdings, Inc., which ultimately became the parent of PayPal, Inc. and holds directly or indirectly all of the assets and liabilities associated with PayPal, Inc. Unless otherwise expressly stated or the context otherwise requires, references to “we,” “our,” “us,” “the Company,” or “PayPal” refer to PayPal Holdings, Inc. and its consolidated subsidiaries or, in the cas of information as of dates or for periods prior to our separation from eBay, the consolidated entities of the payments business of eBay, including PayPal, Inc. and certain other assets and liabilities that were historically held at the eBay corporate level, but were specifically identifiable and attributable to the payments business, and references to our “Payments Platform” mean our combined payment solution capabilities, including our PayPal, PayPal Credit, Braintree, Venmo, Xoom, and iZettle products.

References in this Annual Report on Form 10-K to “eBay” refer to eBay Inc., a Delaware corporation, and its consolidated subsidiaries, which prior to the separation and distribution, but not after such date, included the business and operations of PayPal.

Trademarks, Trade Names and Service Marks

PayPal owns or has rights to use the trademarks, service marks, and trade names that it uses in conjunction with the operation of its business. Some of the more important trademarks that PayPal owns or has rights to use that appear in this Annual Report on Form 10-K include: PayPal®, PayPal Credit®, Braintree, Venmo, Xoom and iZettle, which may be registered or trademarked in the United States and other jurisdictions. PayPal's rights to some of these trademarks may be limited to select markets. Each trademark, trade name, or service mark of any other company appearing in this Annual Report on Form 10-K is, to PayPal's knowledge, owned by such other company.

Table of Contents

PART I

FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934, including statements that involve expectations, plans or intentions, such as those relating to future business, future results of operations or financial condition, new or planned features or services, or management strategies. You can identify these forward-looking statements by words such as “may,” “will,” “would,” “should,” “could,” “expect,” “anticipate,” “believe,” “estimate,” “intend,” “future,” “opportunity,” “plan,” “project,” “forecast,” and other similar expressions. These forward-looking statements involve risks and uncertainties that could cause our actual results to differ materially from those expressed or implied in our forward-looking statements. Such risks and uncertainties include, among others, those discussed in “Item 1A. Risk Factors” of this Annual Report on Form 10-K, as well as in our consolidated financial statements, related notes, and the other information appearing elsewhere in this report and our other filings with the Securities and Exchange Commission (“SEC”). We do not intend, and undertake no obligation except as required by law, to update any of our forward-looking statements after the date of this report to reflect actual results or future events or circumstances. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements. You should read the information in this report in conjunction with the audited consolidated financial statements and the related notes that appear elsewhere in this report.

ITEM 1. BUSINESS

Overview

PayPal Holdings, Inc. was incorporated in Delaware in January 2015 and is a leading technology platform and digital payments company that enables digital and mobile payments on behalf of consumers and merchants worldwide. PayPal is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy. Our goal is to enable our consumers and merchants to manage and move their money anywhere in the world, anytime, on any platform and using any device. Our combined payment solutions, including our PayPal, PayPal Credit, Braintree, Venmo, Xoom and iZettle products, compose our proprietary Payments Platform.

PayPal’s service enables our customers to send and receive payments. We operate a two-sided network where both merchants and consumers have PayPal accounts with stored balance functionality. Since PayPal serves as a proprietary payment method that is accepted by merchants, we are more than a connection to third-party payment networks. Our service enables the completion of payments on our Payments Platform on behalf of our customers. We offer our customers the flexibility to use their accounts to purchase and receive payment for goods and services, as well as to transfer and withdraw funds. We enable consumers to exchange funds more safely with merchants using a variety of funding sources, which may include a bank account, a PayPal account balance, a PayPal Credit account, a credit or debit card, or other stored value products such as coupons and gift cards. Our PayPal, Venmo and Xoom products also make it safer and simpler for friends and family to transfer funds to each other. We offer merchants an end-to-end payments solution that provides authorization and settlement capabilities, as well as instant access to funds. We help merchants connect with their customers and manage risk. We enable consumers to engage in cross-border shopping and merchants to extend their global reach while reducing the complexity and friction involved in enabling overseas and cross-border trade.

We earn revenues primarily by charging fees for completing payment transactions for our customers and other payment-related services that are typically based on the volume of activity processed on our Payments Platform. Generally, we do not charge consumers to fund or draw from their accounts; however, we generate revenue from

consumers on fees charged for foreign currency exchange. We also earn revenue by providing other value added services which comprise revenue earned through partnerships, our PayPal Credit products, subscription fees, gateway services, and other services that we provide to our merchants and consumers. Our gateway services, which include our Payflow Gateway services and Braintree Gateway services, provide the technology that links a merchant's website to its processing network and merchant account and enables merchants to accept payments online with credit or debit cards.

Table of Contents

Strategy

Our ability to grow revenue is affected by, among other things, consumer spending patterns, merchant and consumer adoption of digital payment methods, the expansion of multiple commerce channels, the growth of mobile devices and merchant and consumer applications on those devices, the growth of consumers globally with internet and mobile access, the pace of transition from cash and checks to digital forms of payment, our share of the digital payments market, and our ability to innovate and bring new products and services that merchants and consumers value. Our strategy to drive growth in our business includes the following:

- Growing our core business: through expanding our global capabilities, customer base and scale, increasing our customers' use of our products and services by better addressing their everyday needs related to accessing, managing and moving money, and expanding the adoption of our solutions by new merchants and consumers;

- Expanding our value proposition for customers: by focusing on trust and simplicity, providing risk management and insights from our two-sided Payments Platform, and being technology and platform agnostic;

- Extending through strategic partnerships: by building new strategic partnerships to provide better experiences for our customers, offering greater choice and flexibility, acquiring new customers, and reinforcing our role in the ecosystem; and

- Seeking new areas of growth: organically and through acquisitions in our existing and new international markets around the world and focusing on innovation both in the digital and physical world.

Key Performance Metrics

We measure the relevance of our products and services to our customers, and therefore the success of our business, through active accounts, payment transactions, and payment volume:

Active Accounts: An active account is an account registered directly with PayPal or a platform access partner that has completed a transaction on our Payments Platform, not including gateway-exclusive transactions, within the past 12 months. A platform access partner is a third party whose customers are provided access to PayPal's Payments Platform through such third party's login credentials. As of December 31, 2018, we had approximately 267 million active accounts across more than 200 markets. A market is a geographic area or political jurisdiction, such as a country, territory, or protectorate, in which we offer some or all of our services. A country, territory, or protectorate is identified by a distinct set of laws and regulations.

Table of Contents

Number of Payment Transactions: Number of payment transactions is the total number of payments, net of payment reversals, successfully completed on our Payments Platform or enabled by PayPal via a partner payment solution, not including gateway-exclusive transactions.

Total Payment Volume ("TPV"): TPV is the value of payments, net of reversals, successfully completed on our Payments Platform or enabled by PayPal via a partner payment solution, not including gateway-exclusive transactions.

Our Strengths

Our business is built on a strong foundation designed to drive growth and differentiate us from our competitors. We believe that our competitive strengths include the following:

- Two-sided Platform—our platform connecting merchants and consumers enables PayPal to offer unique end-to-end product experiences while gaining valuable insights into customer behavior through our data. Our platform provides for simple digital and mobile transactions while being both technology and platform agnostic.

- Scale—our global scale allows us to drive organic growth. As of December 31, 2018, we had 267 million active accounts, which included 21 million active merchant accounts. In 2018, we processed $578 billion of TPV in more than 200 markets around the world.

- Brands—we have built well-recognized and trusted brands. Our marketing efforts play an important role in building brand visibility, usage, and overall preference among customers.

- Risk Management—our risk management system and tokenization usage are designed to help keep our customers safe and to help ensure we process legitimate transactions around the world, while identifying and reducing illegal, high-risk, or fraudulent transactions.

- Regulatory—we believe that our regulatory licenses, which enable us to operate in markets around the world, are a distinct advantage and support business growth.

Technology

Our Payments Platform utilizes a combination of proprietary and third-party technologies and services to efficiently and securely facilitate transactions between millions of merchants and consumers worldwide across different channels, markets and networks. Our Payments Platform connects with financial service providers around the world and allows consumers to make purchases using a wide range of payment methods, regardless of where a merchant is located. Consumers who use our Payments Platform can send payments in more than 200 markets across the globe and in more than 100 currencies, withdraw funds to their bank accounts in 56 currencies and hold balances in their PayPal accounts in 25 currencies.

A transaction on our Payments Platform can involve multiple participants in addition to us, including a merchant, a consumer, and the consumer's funding source provider. We have developed intuitive user interfaces, customer tools, and transaction completion database and network applications on our Payments Platform that help our customers utilize our suite of products and services. Our Payments Platform, open application programming interfaces, and developer tools are designed to enable developers to innovate with ease and offer robust applications to our global ecosystem of merchants and consumers, while at the same time maintaining the security of our customers' financial information.

The technology infrastructure supporting our Payments Platform simplifies the storage and processing of large amounts of data and facilitates the deployment and operation of large-scale global products and services. Our technology infrastructure is designed around industry-standard architectures intended to reduce downtime in the event of outages or catastrophic occurrences. Our Payments Platform incorporates multiple layers of protection for continuity and system redundancy purposes and to help address cybersecurity challenges. We have a comprehensive cybersecurity program designed to protect our technology infrastructure and Payments Platform against these challenges, including regularly testing our systems to address potential vulnerabilities. We strive to continually improve our technology infrastructure and Payments Platform to enhance the customer experience and to increase efficiency, scalability, and security.

Table of Contents

Merchant and Consumer Payment Solutions

Our combined payment solution capabilities offer our merchants and consumers a broad range of products and services, enabling our merchants to securely and simply receive payments from their customers while allowing our consumers to make seamless transactions across different markets and networks.

We partner with our merchants to help grow and expand their businesses by improving sales conversion; providing global reach, offering alternative payment methods; reducing losses through proprietary protection programs, providing fraud prevention and risk management solutions; and leveraging data analytics. We generate revenues from merchants primarily by charging fees for completing their payment transactions and other payment-related services. Merchants can onboard quickly with PayPal and are generally not required to invest in new or specialized hardware. We do not charge merchants setup or recurring fees for our standard service. We offer access to credit products for certain small and medium-sized merchants through our PayPal Working Capital and PayPal Business Loan products, which we collectively refer to as our business financing offerings. Our PayPal Working Capital product allows businesses to borrow a certain percentage of their annual payment volume processed by PayPal for a fixed fee. Our PayPal Business Loan product provides businesses with short-term financing for a fixed fee based on an evaluation of both the applying business as well as the business owner. We believe that our business financing offerings allow us to deepen our engagement with our existing small and medium-sized business merchants and expand services to new merchants by providing access to capital that may not be available effectively or efficiently from traditional banks or other lending providers.

PayPal is a popular form of payment for mobile commerce, and our business has grown with the increased adoption of mobile devices. We believe our Braintree products strengthen our position in mobile payments and extend our coverage to a new class of retailers and service providers that offer their services primarily through mobile applications. Through a single Braintree integration, a merchant can begin accepting payments with credit or debit cards, PayPal, PayPal Credit, Google Pay, Apple Pay, Samsung Pay, and other payment solutions. We also offer gateway services, including our Payflow Gateway services and Braintree Gateway services, which enable merchants to accept payments online with credit or debit cards. Our gateway services provide the payment gateway technology that links a merchant’s website to its processing network and enable merchants to accept payments online with credit and debit cards.

We believe that our recent acquisition of iZettle in September 2018 will enable us to further expand our in-store presence and strengthen our Payments Platform to help small businesses around the world grow and thrive in an omnichannel retail environment. iZettle offers a card acceptance service that enables small businesses to take credit and debit card payments, as well as a software solution to record, manage and analyze sales. iZettle provides in-store capabilities in eleven countries, as well as near-term, in-store expansion opportunities into other existing PayPal markets.

We focus on providing affordable consumer products intended to democratize the management and movement of money. We generate revenue from consumers on fees charged for foreign currency exchange and on interest and fees from our PayPal Credit product. We offer our PayPal Credit product to consumers as a potential funding source at checkout. Once a consumer is approved for credit, PayPal Credit is made available as a funding source in his or her account. We believe that our consumer credit products allow us to increase engagement with consumers and merchants on our two-sided network and differentiate ourselves from other payment processors by helping merchants drive incremental sales through products like PayPal Credit. We are responsible for servicing functions related to all of our credit products. In the U.S., credit originating from our PayPal Working Capital and PayPal Business Loan products is currently extended through third-party financial institutions from whom we purchase the related receivables. For our consumer and merchant credit products outside the U.S., we extend credit through certain international PayPal subsidiaries.

During the fourth quarter of 2017, we expanded our strategic consumer credit relationship with Synchrony Financial and agreed to sell our U.S. consumer credit receivables portfolio to Synchrony Bank. Following the closing of this transaction in July 2018, Synchrony Bank became the exclusive issuer of the U.S. PayPal branded consumer credit program and we no longer hold an ownership interest in receivables generated through the program.

We offer consumers person-to-person ("P2P") payment solutions through our PayPal, Venmo and Xoom products. PayPal continues to be a key driver of our total P2P volumes, enabling both domestic and international P2P transfers across our Payments Platform. Our Venmo app in the U.S. is a leading mobile application used to move money between our customers and to make purchases at approved merchants. Xoom is an international money transfer service that enables our customers to send money to, pay bills for, and send prepaid mobile phone reloads to people around the world in a secure, fast, and cost-effective way, using a mobile device or personal computer. P2P is a significant customer acquisition channel that facilitates organic growth by enabling potential PayPal users to establish active accounts with us at the time they make or receive a P2P payment.

Table of Contents

Protecting Merchants and Consumers

Protecting merchants and consumers on our Payments Platform from financial and fraud loss is imperative to successfully competing in the payments industry and sustainably growing our business. Fraudulent activities, such as account takeover, identity theft, and counterparty malicious activities, represent a significant risk to merchants and consumers, as well as their payment partners. We provide merchants and consumers with protection programs on most purchase transactions completed on our Payments Platform, excluding gateway-exclusive transactions or situations where our customer agreements specifically do not provide for protections. We believe that these programs, which protect both merchants and consumers from financial and fraud loss due primarily to fraud and counterparty non-performance, are generally much broader than similar protections provided by other participants in the payments industry. As a result, merchants may incur losses for chargebacks and other claims on certain transactions when using other payments providers that the merchants would not incur if they used our payments services. We also provide consumer protection against losses on qualifying purchases and accept claims for review up to 180 days post-transaction. We believe that this protection is generally consistent with, or better than, that offered by other payments providers. These programs are designed to promote confidence on both the part of consumers (i.e., when using our Payment Platform, they will only be required to pay if they receive their purchased item or service in the condition significantly as described) and merchants (i.e., they will receive payment for the product they deliver to the customer).

Our ability to protect both consumers and merchants is based largely on our proprietary, end-to-end Payments Platform and our ability to leverage the data from both sides of transactions on our two-sided network (i.e., from buyers and sellers, and from senders and receivers of payments). We believe mobile devices will continue to play a significant and increasing role in commerce, including by creating the opportunities to make our ecosystem safer. For example, PayPal is able to use location data from mobile devices and growing protection for the mobile operating environment to reduce financial and fraud risk to merchants and consumers. Our ongoing investment in systems and processes, designed to enhance the safety and security of our products, reflects our goal of having PayPal recognized as one of the world’s most trusted payments brands.

Competition

The global payments industry is highly competitive, rapidly changing, highly innovative, and increasingly subject to regulatory scrutiny and oversight. We compete against a wide range of businesses, including those that are larger than we are, have a dominant and secure position, or offer other products and services to consumers and merchants that we do not offer, as well as smaller companies that may be able to respond more quickly in the face of regulatory and technological changes. We compete against all forms of payments, including credit and debit cards; automated clearing house and bank transfers; other online payment services; mobile payments; and offline payment methods, including cash and check.

We compete primarily on the basis of the following:

- ability to attract, retain, and engage both merchants and consumers with our two-sided platform;
- ability to demonstrate to merchants that they may achieve incremental sales by using and offering our services to consumers;
- consumer confidence in the safety and security of transactions on our Payments Platform, including the ability for consumers to use our products and services without sharing their financial information with the merchant or any other party they are paying;
- simplicity and transparency of our fee structure;
- ability to develop products and services across multiple commerce channels, including mobile payments, credit products, and payments at the retail point of sale;

- trust in our dispute resolution and buyer and seller protection programs;
- customer service experience;
- brand recognition and preference;
- website, mobile platform and application onboarding, ease-of-use, speed, availability, and dependability;
- the technology and payment agnostic nature of our Payments Platform;
- system reliability and data security;
- ability to assist merchants in complying with payments-related laws and regulations ;
- ease and quality of integration into third-party mobile applications and operating systems; and
- quality of developer tools, such as our application programming interfaces and software development kits.

In addition to the discussion in this section, see “Item 1A. Risk Factors” under the caption “We face substantial and increasingly intense competition worldwide in the global payments industry” for further discussion of the potential impact of competition on our business.

Table of Contents

Research and Development

Total research and development expense was $1.1 billion, $953 million and $834 million in 2018, 2017 and 2016, respectively.

Intellectual Property

The protection of our intellectual property, including our trademarks (particularly those covering the PayPal name), patents, copyrights, domain names, trade dress, and trade secrets is important to the success of our business. We seek to protect our intellectual property rights by relying on applicable laws and regulations in the U.S. and internationally, as well as a variety of administrative procedures. We also rely on contractual restrictions to protect our proprietary rights when offering or procuring products and services. We have routinely entered into confidentiality and invention assignment agreements with our employees and contractors, and non-disclosure agreements with parties with whom we conduct business, to control use, access to, and limit disclosure of our proprietary information.

We pursue the registration of our domain names, trademarks, and service marks in the U.S. and internationally. Additionally, we have filed patent applications in the U.S. and in international jurisdictions covering certain aspects of our proprietary technology and new innovations. We have registered our core brands as domain names and as trademarks in the U.S. and a large number of other jurisdictions. We also have in place an active program to continue to secure and enforce trademarks and domain names that corresponds to our brands in markets of interest.

For additional information regarding some of the risks relating to our intellectual property, including costs of protecting our intellectual property, see the information in “Item 1A. Risk Factors” under the captions “We are subject to patent litigation” and “We may be unable to adequately protect or enforce our intellectual property rights, or third parties may allege that we are infringing their intellectual property rights.”

Government Regulation

We operate globally and in a rapidly evolving regulatory environment characterized by a heightened regulatory focus on all aspects of the payments industry. That focus continues to become even more heightened as regulators on a global basis focus on such important issues as countering terrorist financing, anti-money laundering, privacy, cybersecurity, and consumer protection. Some of the laws and regulations to which we are subject were enacted recently, and the laws and regulations applicable to us, including those enacted prior to the advent of digital and mobile payments, are continuing to evolve through legislative and regulatory action and judicial interpretation. New or changing laws and regulations, including how such laws and regulations are interpreted and implemented, as well as increased penalties and enforcement actions related to non-compliance, could have a material adverse impact on our business, results of operations, and financial condition. Therefore, we monitor these areas closely to design compliant solutions for our customers who depend on us.

Government regulation impacts key aspects of our business. We are subject to regulations that affect the payments industry in the markets we operate.

Payments Regulation. Various laws and regulations govern the payments industry in the U.S. and internationally. In the U.S., PayPal, Inc. holds licenses to operate as a money transmitter (or its equivalent), which, among other things, subjects PayPal, Inc. to reporting requirements, bonding requirements, limitations on the investment of customer funds, and inspection by state regulatory agencies. Outside the U.S., we provide similar services customized for various countries and foreign jurisdictions through our foreign subsidiaries. The activities of those non-U.S. entities are, or may be, supervised by a financial regulatory authority in the jurisdictions in which they operate. Among other regulatory authorities, the Luxembourg Commission de Surveillance du Secteur Financier (the “CSSF”), the Australian

Securities and Investment Commission, the Monetary Authority of Singapore, the Reserve Bank of India, and the Central Bank of Russia have asserted jurisdiction over some or all of our activities in their respective jurisdictions. This list is not exhaustive, and there are numerous other regulatory agencies that have or may assert jurisdiction over our activities. The laws and regulations applicable to the payments industry in any given jurisdiction are subject to interpretation and change.

Banking Agency Supervision. We serve our customers in the European Union ("EU") through PayPal (Europe) S.à.r.l. et Cie, SCA, a wholly-owned subsidiary that is licensed and subject to regulation as a bank in Luxembourg by the CSSF. Consequently, we must comply with rules and regulations of the European banking industry, including those related to capitalization, funds management, corporate governance, anti-money laundering, disclosure, reporting, and inspection. We also are, or may be, subject to banking-related regulations in other countries now or in the future related to our role in the financial industry. In addition, based on our relationships with our partner financial institutions, we are, or may be, subject to indirect regulation and examination by these financial institutions' regulators.

Table of Contents

Consumer Financial Protection Bureau. The Consumer Financial Protection Bureau (the "CFPB") has significant authority to regulate consumer financial products in the U.S., including consumer credit, deposit, payment, and similar products. As a large market participant of remittance transfers, the CFPB has direct supervisory authority over our business. The CFPB and other similar regulatory agencies in other jurisdictions may have broad consumer protection mandates that could result in the promulgation and interpretation of rules and regulations that may affect our business.

Anti-Money Laundering and Counter-Terrorist Financing. PayPal is subject to anti-money laundering ("AML") laws and regulations in the U.S. and other jurisdictions, as well as laws designed to prevent the use of the financial systems to facilitate terrorist activities. Our AML program is designed to prevent our payment network from being used to facilitate money laundering, terrorist financing, and other illicit activities, or to do business in countries or with persons and entities included on designated country or person lists promulgated by the U.S. Department of the Treasury's Office of Foreign Assets Controls ("OFAC") and equivalent authorities in other countries. Our AML and sanctions compliance programs, overseen by our AML/Bank Secrecy Act Officer, is composed of policies, procedures and internal controls, and is designed to address these legal and regulatory requirements and assist in managing money laundering and terrorist financing risks.

Interchange Fees. Interchange fees associated with four-party payments systems are being reviewed or challenged in various jurisdictions. For example, in the EU, the Multilateral Interchange Fee ("MIF") Regulation caps credit and debit interchange fees for card payments and provides for business rules to be complied with by any company dealing with card transactions, including PayPal. As a result, the fees that we collect in certain jurisdictions may become the subject of regulatory challenge.

Data Protection and Information Security. Aspects of our operations or business are subject to privacy and data protection regulation in the U.S., the EU, Asia Pacific, and elsewhere. For example, the EU adopted a comprehensive General Data Protection Regulation (the "GDPR"), which came into effect in May 2018, as supplemented by any national laws (such as in the U.K., the Data Protection Act 2018) and further implemented through binding guidance from the European Data Protection Board,and expanded the scope of the EU data protection law to foreign companies processing personal data of European Economic Area ("EEA") individuals, imposed a stricter data protection compliance regime, and included new data subject rights (e.g., the right to erasure, commonly known as the "right to be forgotten"). In the U.S., we are subject to privacy information safeguarding requirements under the Gramm-Leach-Bliley Act that require the maintenance of a written, comprehensive information security program and in Europe, the operations of our Luxembourg bank are subject to confidentiality and information safeguarding requirements under the Luxembourg Banking Act, among other laws. Regulatory authorities around the world are considering numerous legislative and regulatory proposals concerning privacy and data protection that may contain additional privacy and data protection obligations than exist today. In addition, the interpretation and application of these privacy and data protection laws in the U.S., Europe and elsewhere are often uncertain and in a state of flux.

Anti-Corruption. PayPal is subject to applicable anti-corruption laws, such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act, and similar anti-corruption laws in the jurisdictions in which we operate. Anti-corruption laws generally prohibit offering, promising, giving, accepting, or authorizing others to provide anything of value, either directly or indirectly, to or from a government official or private party in order to influence official action or otherwise gain an unfair business advantage, such as to obtain or retain business. We have implemented policies, procedures, and internal controls that are designed to comply with these laws and regulations.

Additional Regulatory Developments. Various regulatory agencies continue to examine a wide variety of issues, including virtual currencies, identity theft, account management guidelines, privacy, disclosure rules, cybersecurity, and marketing that may impact PayPal's business.

For an additional discussion on governmental regulation affecting our business, please see the risk factors related to regulation of our payments business and regulation in the areas of consumer privacy, data use, and/or security in “Item 1A. Risk Factors” under the caption “Risk Factors That May Affect Our Business, Results of Operations and Financial Condition” and “Item 3. Legal Proceedings” included elsewhere in this Annual Report on Form 10-K.

Seasonality

The Company does not experience meaningful seasonality with respect to net revenues. No individual quarter in 2018, 2017 or 2016 accounted for more than 30% of annual net revenue.

Table of Contents

Employees

As of December 31, 2018, we employed approximately 21,800 people globally, of whom approximately 11,500 were located in the U.S. We consider our relationship with our employees to be good.

Separation from eBay Inc.

PayPal Holdings, Inc. was incorporated in Delaware in January 2015 for the purpose of owning and operating eBay's Payments business in connection with the separation and distribution described below. Prior to the contribution of this business to PayPal Holdings, Inc., which occurred prior to the distribution in July 2015, PayPal Holdings, Inc. had no operations. On July 17, 2015 (the "distribution date"), PayPal became an independent publicly traded company through the pro rata distribution by eBay of 100% of the outstanding common stock of PayPal to eBay stockholders (which we refer to as the "separation" or the "distribution"). Each eBay stockholder of record as of the close of business on July 8, 2015 received one share of PayPal common stock for every share of eBay common stock held on the record date. Approximately 1.2 billion shares of PayPal common stock were distributed on July 17, 2015 to eBay stockholders. PayPal's common stock began "regular way" trading under the ticker symbol "PYPL" on the NASDAQ Stock Market on July 20, 2015. Prior to the separation, eBay transferred substantially all of the assets and liabilities and operations of eBay's payments business to PayPal, which was completed in June 2015.

Available Information

The address of our principal executive offices is PayPal Holdings, Inc., 2211 North First Street, San Jose, California 95131. Our website is located at www.paypal.com, and our investor relations website is located at http://investor.paypal-corp.com. From time to time, we may use our investor relations site and other online and social media channels, including our PayPal Stories Blog (https://www.paypal.com/stories/us), Twitter handles (@PayPal and @PayPalNews), LinkedIn page (https://www.linkedin.com/company/paypal), Facebook page (https://www.facebook.com/PayPalUSA/), YouTube channel (https://www.youtube.com/paypal), Dan Schulman's LinkedIn profile (https://www.linkedin.com/in/dan-schulman/), John Rainey's LinkedIn profile (www.linkedin.com/in/john-rainey-pypl), Bill Ready's LinkedIn profile (https://www.linkedin.com/in/williamready/), and Dan Schulman's Facebook page (https://www.facebook.com/DanSchulmanPayPal/) to disclose material non-public information and comply with our disclosure obligations under Regulation Fair Disclosure. Our Annual Report on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, and amendments to those reports are available free of charge on our investor relations website as soon as reasonably practicable after they are electronically filed with, or furnished to, the SEC. The content of our websites and information we may post on or provide to online and social media channels, including those mentioned above, and information that can be accessed through our websites or these online and social media channels is not incorporated by reference into this Annual Report on Form 10-K or in any other report or document we file with the SEC, and any references to our websites or these online and social media channels are intended to be inactive textual references only.

ITEM 1A. RISK FACTORS

The following discussion is divided into three sections. The first section, which begins immediately following this paragraph, discusses some of the risks that may adversely affect our business, results of operations and financial condition. The second section, captioned "Risks Related to Our Separation from eBay" discusses some of the risks relating to our separation from eBay in July 2015 into an independent publicly traded company. The third section, captioned "Risks Related to Our Common Stock," discusses some of the risks relating to an investment in our Common Stock. You should carefully review all of these sections in addition to the other information appearing in this Annual Report on Form 10-K, including our consolidated financial statements and related notes, for important information regarding risks and uncertainties that affect us. The risks and uncertainties described below are not the only ones we

face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, may also become important factors that adversely affect our business. If any of the following risks actually occur, our business, financial condition, results of operations, and future prospects could be materially and adversely affected.

Table of Contents

Risk Factors That May Affect Our Business, Results of Operations, and Financial Condition

We face substantial and increasingly intense competition worldwide in the global payments industry.

The global payments industry is highly competitive, rapidly changing, highly innovative, and increasingly subject to regulatory scrutiny. We compete against a wide range of businesses, including businesses that are larger than we are, have a more dominant and secure position, or offer other products and services to consumers and merchants that we do not offer, as well as smaller companies that may be able to respond more quickly to regulatory and technological changes. Many of the areas in which we compete evolve rapidly with changing and disruptive technologies, shifting user needs, and frequent introductions of new products and services. Competition may also intensify as businesses enter into business combinations and alliances, and established companies in other segments expand to become competitive with different aspects of our business.

We compete primarily on the basis of the following:

- ability to attract, retain, and engage both merchants and consumers with our two-sided platform;
- ability to demonstrate to merchants that they may achieve incremental sales by using and offering our services to consumers;
- consumer confidence in the safety and security of transactions on our Payments Platform, including the ability for consumers to use our products and services without sharing their financial information with the merchant or any other party they are paying;
- simplicity and transparency of our fee structure;
- ability to develop products and services across multiple commerce channels, including mobile payments, credit products, and payments at the retail point of sale;
- trust in our dispute resolution and buyer and seller protection programs;
- customer service experience;
- brand recognition and preference;
- website, mobile platform and application onboarding, ease-of-use, speed, availability, and dependability;
- the technology and payment agnostic nature of our Payments Platform;
- system reliability and data security;
- ability to assist merchants in complying with payments-related laws and regulations ;
- ease and quality of integration into third-party mobile applications and operating systems; and
- quality of developer tools, such as our application programming interfaces and software development kits.

We compete against a wide range of businesses with varying roles in all forms of payments, including:

- paper-based transactions (principally cash and checks);
- providers of traditional payment methods, particularly credit and debit cards and Automated Clearing House transactions (in particular, well-established banks);
- payment networks which facilitate payments for credit card users;
- providers of “digital wallets” which offer customers the ability to pay online and/or in-store through a variety of payment methods, including with mobile applications, through contactless payments, and with a variety of payment cards;
- providers of mobile payments solutions that use tokenized card data approaches and contactless payments (e.g., near field communication (“NFC”) or host card emulation functionality) to eliminate the need to swipe or insert a card or enter a personal identification number or password;
- payment-card processors that offer their services to merchants, including for “card on file” payments where the merchant invites the consumer to select a payment method for their first transaction and to use the same payment

method for subsequent transactions;
- providers of “person-to-person” payments that facilitate individuals sending money with an email address or mobile phone number;
- merchants and merchant associations providing proprietary payment networks to facilitate payments within their own retail network;
- money remitters;
- providers of card readers for mobile devices and of other point-of-sale and multi-channel technologies; and
- providers of virtual currencies and distributed ledger technologies.

We often partner with many of these businesses and we consider the ability to continue establishing these partnerships as important to our business. Competition for relationships with these partners is intense and there can be no assurance that we will be able to continue to establish, grow, or maintain these partner relationships.

Table of Contents

We also face competition and potential competition from:

- service providers that provide online merchants the ability to offer their customers the option of paying for purchases from their bank account or paying on credit;
- issuers of stored value products targeted at online payments;
- other global online and mobile payment-services providers;
- services targeting users of social networks and online gaming, including those offering social commerce and peer-to-peer payments;
- payment services enabling banking customers to send and receive payments through their bank account, including through immediate or real-time payments systems;
- ecommerce services that provide special offers linked to a specific payment provider;
- services that help merchants accept and manage virtual currencies; and
- electronic funds transfer services as a method of payment for both online and offline transactions.

Some of these competitors have larger customer bases, volume, scale, resources, and market share than we do, which may provide them significant competitive advantages. Some of our competitors may also be subject to less burdensome licensing, anti-money laundering, counter-terrorist financing, and other regulatory requirements. They may devote greater resources to the development, promotion, and sale of products and services, and they may offer lower prices or more effectively introduce their own innovative programs, products, and services that adversely impact our growth.

If we are not able to differentiate our products and services from those of our competitors, drive value for our customers, or effectively align our resources with our goals and objectives, we may not be able to compete effectively in the market.

Substantially all of our net revenues each quarter come primarily from transactions involving payments during that quarter, which may result in significant fluctuations in our operating results that could adversely affect our business, financial condition, results of operations, and cash flows, as well as the trading price of our common stock.

Substantially all of our net revenues each quarter come primarily from transactions involving payments during that quarter. As a result, our operating and financial results have varied on a quarterly basis during our operating history, and may continue to fluctuate significantly as a result of a variety of factors, including as a result of the risks set forth in this “Risk Factors” section. It is difficult for us to forecast accurately the level or source of our revenues or earnings. In view of the rapidly evolving nature of our business, period-to-period comparisons of our operating results may not be meaningful, and you should not rely upon them as an indication of future performance. Due to the inherent difficulty in forecasting revenues, it is also difficult to forecast expenses as a percentage of net revenues. Quarterly and annual expenses as a percentage of net revenues reflected in our financial statements may be significantly different from historical or projected rates. Our operating results in one or more future quarters may fall below the expectations of securities analysts and investors. The trading price of our common stock may decline significantly as a result of the factors described in this paragraph.

Global and regional economic conditions could harm our business.

Our operations and performance depend significantly on global and regional economic conditions. Uncertainty about global and regional economic events and conditions may result in consumers and businesses postponing or lowering spending in response to, among other factors:

- tighter credit,
- higher unemployment,

- consumer debt levels or reduced consumer confidence.
- financial market volatility,
- fluctuations in foreign currency exchange rates and interest rates,
- changes and uncertainties related to government fiscal and tax policies, including increased duties, tariffs, or other restrictions,
- the inability of the U.S. Congress to enact a budget in a fiscal year, another sequestration, and/or another shutdown of the U.S. government,
- government austerity programs, and
- other negative financial news or macroeconomic developments.

Table of Contents

These and other global and regional economic events and conditions, including Brexit, could have a material adverse impact on the demand for our products and services, including a reduction in the volume and size of transactions on our Payments Platform. In addition, any financial turmoil affecting the banking system or financial markets could cause additional consolidation of the financial services industry, significant financial service institution failures, new or incremental tightening in the credit markets, low liquidity, and extreme volatility or distress in the fixed income, credit, currency, and equity markets, which could have a material adverse impact on our business. See also the risk factor captioned, “The United Kingdom's departure from the EU could adversely affect us.”

If we cannot keep pace with rapid technological developments to provide new and innovative products and services, the use of our products and services and, consequently, our revenues could decline.

Rapid, significant, and disruptive technological changes impact the industries in which we operate, including developments in payment card tokenization, cryptocurrencies, mobile, social commerce (i.e., ecommerce through social networks), authentication, virtual currencies (including distributed ledger and blockchain technologies), and NFC and other proximity payment technology, such as contactless payments. As a result, we expect new services and technologies to continue to emerge and evolve, and we cannot predict the effects of technological changes on our business. In addition to our own initiatives and innovations, we rely in part on third parties, including some of our competitors, for the development of and access to new or evolving technologies. These third parties may restrict or prevent our access to, or utilization of, those technologies, as well as their platforms or products. In addition, we may not be able to accurately predict which technological developments or innovations will become widely adopted and how those technologies may be regulated. We expect that new services and technologies applicable to the industries in which we operate will continue to emerge and may be superior to, or render obsolete, the technologies we currently use in our products and services. Developing and incorporating new technologies into our products and services may require substantial expenditures, take considerable time, and ultimately may not be successful. In addition, our ability to adopt new products and services and to develop new technologies may be inhibited by industry-wide standards, payments networks, changes to laws and regulations, resistance to change from consumers or merchants, third-party intellectual property rights, or other factors. Our success will depend on our ability to develop and incorporate new technologies and adapt to technological changes and evolving industry standards; if we are unable to do so in a timely or cost-effective manner, our business could be harmed.

Cyberattacks and security vulnerabilities could result in serious harm to our reputation, business, and financial condition.

Our business involves the collection, storage, processing, and transmission of customers’ personal data, including financial information and information about how they interact with our Payments Platform. In addition, a significant number of our customers authorize us to bill their payment cards or bank accounts directly for all transaction and other fees charged by us. We have built our reputation on the premise that our Payments Platform offers customers a more secure way to make payments. An increasing number of organizations, including large merchants, businesses, technology companies, and financial institutions, as well as government institutions, have disclosed breaches of their information security systems, some of which have involved sophisticated and highly targeted attacks, including on their websites, mobile applications, and infrastructure.

The techniques used to obtain unauthorized, improper, or illegal access to our systems, our data or customers' data, disable or degrade service, or sabotage systems are constantly evolving and have become increasingly complex and sophisticated, may be difficult to detect quickly, and often are not recognized or detected until after they have been launched against a target. We expect that unauthorized parties will continue to attempt to gain access to our systems or facilities through various means, including hacking into our systems or facilities or those of our customers, partners, or vendors, or attempting to fraudulently induce (for example, through spear phishing attacks) our employees, customers, partners, vendors, or other users of our systems into disclosing user names, passwords, payment card

information, or other sensitive information, which may in turn be used to access our information technology systems. Certain efforts may be state-sponsored and supported by significant financial and technological resources, making them even more sophisticated and difficult to detect. Numerous and evolving cybersecurity threats, including advanced and persisting cyberattacks, phishing and social engineering schemes, could compromise the confidentiality, availability, and integrity of the data in our systems. We believe that PayPal is a particularly attractive target for such breaches and attacks due to our name and brand recognition and the widespread adoption and use of our products and services. Although we have developed systems and processes designed to protect our data and customer data and to prevent data loss and other security breaches, and expect to continue to expend significant resources to bolster these protections, there can be no assurance that these security measures provide absolute security.

Our information technology and infrastructure may be vulnerable to cyberattacks or security breaches, and third parties may be able to access our customers' personal or proprietary information and payment card data that are stored on or accessible through those systems. We have experienced from time to time, and may experience in the future, breaches of our security measures due to human error, malfeasance, system errors or vulnerabilities, or other irregularities. Actual or perceived breaches of our security could, among other things:

Table of Contents

- interrupt our operations,
- result in our systems or services being unavailable,
- result in improper disclosure of data,
- materially harm our reputation and brands,
- result in significant regulatory scrutiny and legal and financial exposure,
- cause us to incur significant remediation costs,
- lead to loss of customer confidence in, or decreased use of, our products and services,
- divert the attention of management from the operation of our business,
- result in significant compensation or contractual penalties from us to our customers and their business partners as a result of losses to them or claims by them, and
- adversely affect our business and results of operations.

In addition, any cyberattacks or data security breaches affecting companies that we acquire or our customers, partners, or vendors (including data center and cloud computing providers) could have similar negative effects. See Note 4—"Business Combinations," Note 5—"Goodwill and Intangible Assets" and Note 13—"Commitments and Contingencies" to consolidated financial statements for disclosure relating to the suspension of operations of TIO Networks ("TIO") (which we acquired in July 2017) as part of an investigation of security vulnerability of the TIO platform. Actual or perceived vulnerabilities or data breaches have led and may lead to claims against us.

In addition, 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 our direct payment card processing vendors, we could be liable to the payment card issuing banks for their cost of issuing new cards and related expenses. We also expect to expend significant additional resources to protect against security or privacy breaches, and may be required to redress problems caused by breaches. Financial services regulators in various jurisdictions, including the U.S. and the EU, have implemented authentication requirements for banks and payment processors intended to reduce online fraud, which could impose significant costs, require us to change our business practices, make it more difficult for new customers to join PayPal, and reduce the ease of use of our products, which could harm our business. While we maintain insurance policies, they may not be adequate to reimburse us for losses caused by security breaches.

Systems failures and resulting interruptions in the availability of our websites, applications, products, or services could harm our business.

Our systems and those of our services providers and partners may experience service interruptions or degradation because of hardware and software defects or malfunctions, distributed denial-of-service and other cyberattacks, human error, earthquakes, hurricanes, floods, fires, and other natural disasters, power losses, disruptions in telecommunications services, fraud, military or political conflicts, terrorist attacks, computer viruses or other malware, or other events. We have experienced from time to time, and may experience in the future, disruptions in our systems due to break-ins, sabotage, and intentional acts of vandalism. Some of our systems are not fully redundant, and our disaster recovery planning may not be sufficient for all eventualities. In addition, as a provider of payments solutions, we are subject to heightened scrutiny by regulators that may require specific business continuity, resiliency and disaster recovery plans, and more rigorous testing of such plans, which may be costly and time-consuming and may divert our resources from other business priorities.

We have experienced and expect to continue to experience system failures, denial-of-service attacks, and other events or conditions from time to time that interrupt the availability, or reduce or adversely affect the speed or functionality of our products and services. These events have resulted and likely will result in loss of revenue. A prolonged interruption in the availability or reduction in the availability, speed, or functionality of our products and services could materially harm our business. Frequent or persistent interruptions in our services could cause current or

potential customers to believe that our systems are unreliable, leading them to switch to our competitors or to avoid or reduce the use of our products and services, and could permanently harm our reputation and brands. Moreover, if any system failure or similar event results in damages to our customers or their business partners, these customers or partners could seek significant compensation or contractual penalties from us for their losses, and those claims, even if unsuccessful, would likely be time-consuming and costly for us to address, and could have other consequences described in this "Risk Factors" section under the caption "Cyberattacks and security vulnerabilities could result in serious harm to our reputation, business, results of operation, and financial condition."

Table of Contents

Our Payments Platform has experienced and may in the future experience intermittent unavailability. The full-time availability and expeditious delivery of our products and services is critical to our goal of gaining widespread acceptance among consumers and merchants for digital payments. We have undertaken certain system upgrades and re-platforming efforts designed to improve our reliability and speed. These efforts are costly and time-consuming, involve significant technical risk and may divert our resources from new features and products, and there can be no guarantee that these efforts will succeed. Because we are a regulated financial institution in certain jurisdictions, frequent or persistent site interruptions could lead to regulatory scrutiny, significant fines and penalties, and mandatory and costly changes to our business practices, and ultimately could cause us to lose existing licenses that we need to operate or prevent or delay us from obtaining additional licenses that may be required for our business.

We also rely on facilities, components, and services supplied by third parties, including data center facilities and cloud storage services. If these third parties cease to provide the facilities or services, experience operational interference or disruptions, breach their agreements with us, fail to perform their obligations and meet our expectations, or experience a cybersecurity incident, our operations could be disrupted or otherwise negatively affected, which could result in customer dissatisfaction and damage to our reputation and brands, and materially and adversely affect our business. We do not carry business interruption insurance sufficient to compensate us for all losses that may result from interruptions in our service as a result of systems failures and similar events.

In addition, we are continually improving and upgrading our information systems and technologies. Implementation of new systems and technologies is complex, expensive, and time-consuming. If we fail to timely and successfully implement new information systems and technologies, or improvements or upgrades to existing information systems and technologies, or if such systems and technologies do not operate as intended, this could have an adverse impact on our business, internal controls (including internal controls over financial reporting), results of operations, and financial condition.

Changes to payment card networks or bank fees, rules, or practices could harm our business.

We rely on banks or other payment processors to process transactions and pay fees for their services. From time to time, payment card networks have increased, and may continue to increase in the future, the interchange fees and assessments that they charge for each transaction that accesses their networks. Payment card networks have imposed, and may impose in the future, special fees or assessments for transactions that are executed through a “digital wallet” such as PayPal’s, which could particularly impact us and significantly increase our costs. Our payment card processors may have the right to pass any increases in interchange fees and assessments on to us as well as increase their own fees for processing, which could increase our operating costs and reduce our operating income. We have entered into strategic partnerships with Visa and Mastercard and other credit card networks to further expand our relationships in a way that will make it easier for merchants to accept and consumers to choose to pay with their respective credit and debit cards. During the terms of these agreements, Visa and Mastercard have each agreed to not enact or impose any fees or rules that solely target PayPal. Upon termination of the agreements, PayPal could become subject to special digital wallet fees or other special assessments.

In addition, in some jurisdictions, governmental regulations have required payment card networks to reduce interchange fees. Any material change in credit or debit card interchange rates in the U.S. or other markets, including as a result of changes in interchange fee limitations, could adversely affect our competitive position against traditional credit and debit card service providers and our business.

We are required to comply with payment card network operating rules, including special operating rules for payment service providers to merchants. We have agreed to reimburse our processors for any fines they are assessed by payment card networks as a result of any rule violations by us or our merchants. We may also be directly liable to the payment card networks for rule violations. The payment card networks set and interpret the card operating rules and

have alleged from time to time that various aspects of our business model violate these operating rules. If such allegations are not resolved favorably, they may result in significant fines and penalties or require changes in our business practices that may be costly. The payment card networks could adopt new operating rules or interpret or re-interpret existing rules that we or our processors might find difficult or even impossible to follow, or costly to implement. As a result, we could lose our ability to give consumers the option of using payment cards to fund their payments or the choice of currency in which they would like their payment card to be charged. If we are unable to accept payment cards or are limited in our ability to do so, our business would be adversely affected.

Table of Contents

We and our payment card processors have implemented specific business processes for merchants to comply with payment card network operating rules for providing services to merchants. Any failure to comply with these rules could result in fines. We are also subject to fines from payment card networks if we fail to detect that merchants are engaging in activities that are illegal or that are considered “high risk,” including the sale of certain types of digital content. For “high risk” merchants, we must either prevent such merchants from using PayPal services or register such merchants with the payment card networks and conduct additional monitoring with respect to such merchants. Although the amount of these fines has not been material to date, additional fines in the future could become significant and could result in a termination of our ability to accept payment cards or require changes in our process for registering new customers, which would adversely affect our business. Payment card network rules may also increase the cost of, impose restrictions on, or otherwise negatively impact the development of, our retail point-of-sale solutions, which may negatively impact their deployment and adoption.

Failure to deal effectively with fraud, fictitious transactions, bad transactions, and negative customer experiences would increase our loss rate and harm our business, and could severely diminish merchant and consumer confidence in and use of our services.

Our operations process a significant volume and dollar value of transactions on a daily basis. In the event that merchants do not fulfill their obligations to consumers or a merchant's goods or services do not match the merchant’s description, we may incur substantial losses as a result of claims from consumers. We seek to recover such losses from the merchant, but may not be able to recover in full if the merchant is unwilling or unable to pay. In addition, in the event of the bankruptcy or other business interruption of a merchant that sells goods or services in advance of the date of their delivery or use (e.g., airline, cruise or concert tickets, custom-made goods, and subscriptions), we could be liable to the buyers of such goods or services, either through our buyer protection program or through chargebacks on payment cards used by customers to fund their payment. While we have established allowances for transaction losses based on assumptions and estimates that we believe are reasonable to cover such losses incurred as of the reporting date, these reserves may be insufficient.

We also incur substantial losses from claims that the consumer did not authorize the purchase, from customer fraud, from erroneous transactions, and as a result of customers who have closed bank accounts or have insufficient funds in their bank accounts to satisfy payments. In addition, if losses incurred by us related to payment card transactions become excessive, they could potentially result in our losing the right to accept payment cards for payment, which would harm our business. We have taken measures to detect and reduce the risk of fraud, but these measures need to be continually improved and may not be effective against fraud, particularly new and continually evolving forms of fraud or in connection with new product offerings. If these measures do not succeed, our business could be harmed.

We are exposed to fluctuations in foreign currency exchange rates that could materially and adversely affect our financial results.

We have significant operations internationally that are denominated in foreign currencies, including the British Pound, Euro, Australian Dollar, and Canadian Dollar, which subject us to foreign currency risk. The strengthening or weakening of the U.S. dollar versus the British Pound, Euro, Australian Dollar, and Canadian Dollar impacts the translation of our net revenues generated in these foreign currencies into the U.S. dollar. In connection with providing our services in multiple currencies, we may face financial exposure if we incorrectly set our foreign exchange rates or as a result of fluctuations in foreign exchange rates between the times that we set them. Given that we also hold some corporate and customer funds in non-U.S. currencies, our financial results are affected by the remeasurement of these non-U.S. currencies into U.S. dollars. We also have foreign exchange risk on our assets and liabilities denominated in currencies other than the functional currency of our subsidiaries. While we regularly enter into transactions to hedge foreign currency risk for portions of our foreign currency translation and balance sheet exposure, it is impossible to predict or eliminate the effects of this exposure.

Any factors that reduce cross-border trade or make such trade more difficult could harm our business.

Cross-border trade (i.e., transactions where the merchant and consumer are in different countries) is an important source of our revenue and profits. Cross-border transactions generally provide higher revenues and operating income than similar transactions that take place within a single country or market. Cross-border trade also represents our primary (and in some cases, our only) presence in certain important markets.

Table of Contents

Cross-border trade is subject to, and may be negatively impacted by, foreign exchange rate fluctuations. In addition, the interpretation and application of laws of multiple jurisdictions (e.g., the jurisdiction of the merchant and of the consumer) are often extremely complicated in the context of cross-border trade. Changes to or the interpretation and/or application of laws and regulations applicable to cross-border trade could impose additional requirements and restrictions, impose conflicting obligations, and increase the costs associated with cross-border trade. Any factors that increase the costs of cross-border trade for us or our customers or that restrict, delay, or make cross-border trade more difficult or impractical, such as trade policy or higher tariffs, could negatively impact our revenues and profits and harm our business. See also the risk factor captioned, “Global and regional economic conditions could harm our business.”

Changes in how consumers fund their PayPal transactions could harm our business.

We pay transaction fees when consumers fund payment transactions using credit cards, lower fees when consumers fund payments with debit cards, and nominal fees when consumers fund payment transactions by electronic transfer of funds from bank accounts, or from an existing PayPal account balance or through our PayPal branded consumer credit products. Our financial success is sensitive to changes in the rate at which our consumers fund payments using credit and debit cards (collectively, “payment cards”), which can significantly increase our costs. Although we provide consumers with the opportunity to use their existing PayPal account balance to fund payment transactions, some of our consumers may prefer to use payment cards, especially if these payment cards offer features and benefits that are not provided as part of their PayPal accounts. An increase in the portion of our payment volume funded using payment cards or in fees associated with our funding mix, or other events or developments that make it more difficult or costly for us to fund transactions with lower-cost funding options, could materially and adversely affect our financial performance and significantly harm our business.

We have entered into strategic partnerships with major payment card networks and/or issuing banks to promote greater consumer choice and make it easier for merchants to accept and consumers to pay with these partners’ credit and/or debt cards and to allow us to gain access to these partners’ tokenization services for in-store point of sale PayPal transactions. These arrangements may have an uncertain impact on our business. While we anticipate that these and similar strategic partnerships we may enter into in the future will result in an increase in the number of transactions and transaction volume that we process, we also anticipate that a greater percentage of customer transactions will be executed using a payment card, which would likely increase the transaction costs associated with our funding mix, which could adversely affect our business, results of operations, and profitability.

The United Kingdom’s departure from the EU could adversely affect us.

The United Kingdom (“U.K.”) held a referendum in June 2016 in which a majority of voters approved an exit from the European Union (“EU”) (commonly referred to as “Brexit”). In March 2017, the U.K. government initiated the exit process under Article 50 of the Treaty on European Union, which commenced a two-year period expiring on March 29, 2019, after which time the U.K. is expected to leave the EU in the absence of any effective extension to the Article 50 period. Political negotiations are underway; however, there is a significant lack of clarity over the terms of the U.K.'s exit from the EU and the terms of the U.K.'s future relationship with the EU. The U.K.'s financial service regulators are implementing Temporary Permission Regimes that are expected to be put in place by the U.K.'s government to support European Economic Area (“EEA”) financial services firms in continuing to conduct business in the U.K. should the U.K. exit the EU without an agreement.

Brexit could adversely affect U.K., regional (including European), and worldwide economic and market conditions and could contribute to instability in global financial and foreign exchange markets, including volatility in the value of the British Pound and Euro, which in turn could adversely affect us or our customers and companies with which we do business, particularly in the U.K. Brexit could lead to greater restrictions on the supply and availability of goods and

services between the U.K and the EEA region, with the potential inability of U.K. companies to fulfill orders leading in turn to a risk of increased merchant defaults and buyer protection claims. Brexit could also trigger a general deterioration in credit conditions, a downturn in consumer sentiment and overall negative economic growth. Any of these scenarios could have an adverse effect on our business or our customers.

In addition, Brexit could lead to legal uncertainty and increased complexity for financial services firms as national laws and regulations in the U.K. start to diverge from EU laws and regulations. In particular, depending on the terms of Brexit, we may face new regulatory costs and challenges, including the following:

- if we are unable to utilize appropriate authorizations and regulator permissions, our EU operations could lose their ability to offer services on a cross-border basis into the U.K. market and for our U.K. based operations to offer services on a cross-border basis in the EEA markets. For example, our ability to work primarily with the Luxembourg regulator as the lead authority for various aspects of our U.K. operations may also be impacted;

Table of Contents

- we could be required to obtain additional regulatory permissions to operate in the U.K. market, adding costs and potential inconsistency to our business (and, depending on the capacity of the U.K. authorities, the criteria for obtaining permission, and any possible transitional arrangements, there is a risk that our business in the U.K. could be materially affected or disrupted);
- we could be required to comply with regulatory requirements in the U.K. that are in addition to, or inconsistent with, the regulatory requirements of the EU, leading to increased complexity and costs for our EU and UK operations; and
- our ability to attract and retain the necessary human resources in appropriate locations to support the U.K. business and the EU business of PayPal could be adversely impacted.

These and other factors related to Brexit could, individually or in the aggregate, have a material adverse impact on our business, financial condition, and results of operations.

Our business is subject to extensive government regulation and oversight. Our failure to comply with extensive, complex, overlapping, and frequently changing rules, regulations, and legal interpretations could materially harm our business.

Our business is subject to laws, rules, regulations, policies, and legal interpretations in the markets in which we operate, including, but not limited to, those governing:

- banking,
- credit,
- deposit taking,
- cross-border and domestic money transmission,
- prepaid access,
- foreign exchange,
- privacy,
- data protection,
- cybersecurity,
- banking secrecy,
- payment services (including payment processing and settlement services),
- consumer protection,
- economic and trade sanctions,
- anti-money laundering, and
- counter-terrorist financing.

Our success and increased visibility may result in increased regulatory oversight and enforcement and more restrictive rules and regulations that apply to our business.

As we expand and localize our international activities, we have become increasingly 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 customers worldwide, one or more jurisdictions may claim that we or our customers are required to comply with their laws. Laws regulating the internet, mobile, and related technologies outside of the U.S. often impose different, more specific, or even conflicting obligations on us, as well as broader liability. For example, certain transactions that may be permissible in a local jurisdiction may be prohibited by regulations of U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC") or U.S. anti-money laundering or counter-terrorist financing regulations.

Any failure or perceived failure to comply with existing or new laws, regulations, or orders of any governmental authority (including changes to or expansion of the interpretation of those laws, regulations, or orders), including

those discussed in this risk factor, may subject us to significant fines, penalties, criminal and civil lawsuits, forfeiture of significant assets, and enforcement actions in one or more jurisdictions, result in additional compliance and licensure requirements, increase regulatory scrutiny of our business, restrict our operations, and force us to change our business practices, make product or operational changes, or delay planned product launches or improvements. Any of the foregoing could, individually or in the aggregate, harm our reputation, damage our brands and business, and adversely affect our results of operations and financial condition. The complexity of U.S. federal and state regulatory and enforcement regimes, coupled with the global scope of our operations and the evolving global regulatory environment, could result in a single event giving rise to a large number of overlapping investigations and legal and regulatory proceedings by multiple government authorities in different jurisdictions. We have implemented policies and procedures designed to help ensure compliance with applicable laws and regulations, but there can be no assurance that our employees, contractors, or agents will not violate such laws and regulations.

Table of Contents

Payments Regulation

In the U.S., PayPal, Inc. has obtained licenses to operate as a money transmitter (or its equivalent) in the states where such licenses are required, as well as in the District of Columbia, the U.S. Virgin Islands, and Puerto Rico. These licenses include not only the PayPal branded products and services in these states, but also our Braintree, Venmo, and Xoom products and services. We may also maintain such licenses for certain companies that we have recently acquired, such as Hyperwallet. As a licensed money transmitter, PayPal is subject to restrictions with respect to the investment of customer funds, reporting requirements, bonding requirements, and inspection by state regulatory agencies. Accordingly, if we violate these laws or regulations, we could be subject to liability and/or additional restrictions, forced to cease doing business with residents of certain states, forced to change our business practices, or required to obtain additional licenses or regulatory approvals, which could impose substantial costs.

While we currently allow our customers with payment cards to send payments from approximately 200 markets, we allow customers in only approximately half of those markets (including the U.S.) to also receive payments, in some cases with significant restrictions on the manner in which customers can withdraw funds. These limitations may adversely affect our ability to grow our business in these markets.

We principally provide our services to customers in the EU through PayPal (Europe) S.a.r.l. et Cie., SCA (“PayPal (Europe)”), our wholly-owned subsidiary that is licensed and subject to regulation as a credit institution in Luxembourg. Accordingly, PayPal (Europe) is subject to significant fines or other enforcement action if it violates the disclosure, reporting, anti-money laundering, capitalization, fund management, corporate governance, privacy, data protection, information security, banking secrecy, taxation, sanctions, or other requirements imposed on Luxembourg banks. In addition, EU laws and regulations are typically subject to different and potentially inconsistent interpretations by the countries that are members of the EU, which can make compliance more costly and operationally difficult to manage. Moreover, the countries that are EU members may each have different and potentially inconsistent domestic regulations implementing European Directives, including the EU Payment Services Directive and the E-Money Directive, which could make compliance more costly and operationally difficult to manage. The Revised Payment Services Directive (“PSD2”) entered into force in January 2016 and is in the process of being implemented into national legislation, with certain requirements effective January 13, 2018. However, a number of EU member states have not yet fully implemented PSD2 into domestic legislation. Luxembourg, which is the home member state of PayPal (Europe), implemented PSD2 on July 28, 2018. The implementation of PSD2 may negatively affect our business. PSD2 seeks to enable new payment models whereby a newly formed category of regulated payment provider would be able to access bank and payment accounts (including PayPal accounts) for the purposes of accessing account information or initiating a payment on behalf of a customer. Such access could subject us to data security and other legal and financial risks and could create new competitive forces and new types of competitors in the European payments market. PSD2 seeks to regulate more online platforms that handle payments for their sellers. PayPal merchants with affected business models which are not licensed, or which do not benefit from exemptions or integrate a compliant marketplaces solution may not be able to offer PayPal products in the future. PSD2 also imposes new standards (coming into force on September 14, 2019) for payment security and strong customer authentication that may make it more difficult and time consuming to carry out a PayPal transaction, which may adversely impact PayPal’s customer value proposition and its European business.

If the business activities of PayPal (Europe) exceed certain thresholds, or if the European Central Bank (“ECB”) so determines, PayPal (Europe) may be deemed a significant supervised entity such that some activity of PayPal (Europe) could become directly regulated by the ECB rather than the Luxembourg regulator (the “CSSF”), as its national supervisor, which could subject us to additional requirements and would likely increase compliance costs.

In many of the other markets outside the U.S. in which we do business, we serve our customers through PayPal Pte. Ltd., our wholly-owned subsidiary based in Singapore. PayPal Pte. Ltd. is supervised by the Monetary Authority of

Singapore and designated as a holder of a stored value facility, but does not hold a remittance license. As a result, PayPal Pte. Ltd. is not able to offer outbound remittance payments (including donations to charities) from Singapore, and can only offer payments for the purchase of goods and services in Singapore. In many of the markets (other than Singapore) served by PayPal Pte. Ltd., it is unclear and uncertain whether our Singapore-based service is subject only to Singapore law or, if it is subject to the application of local laws, whether such local laws would require a payment processor like us to be licensed as a payments service, bank, financial institution, or otherwise. Payment services legislation currently pending in Singapore may change how PayPal Pte. Ltd is regulated and, if such legislation is passed, our compliance and operating costs will likely increase.

In certain markets outside the U.S. (e.g., Australia), we provide our services to customers through a local subsidiary subject to local regulatory supervision or oversight, which may be the holder of a local payment license, certification, or other authorization. In such markets, we may be subject to significant fines or other enforcement action if we violate applicable reporting, anti-money laundering, capital requirements, privacy, corporation governance, risk management, or any other applicable requirements.

Table of Contents

We have been, and expect to continue to be, required to apply for various licenses, certifications, and regulatory approvals in a number of the jurisdictions where we provide our services, including due to changes in applicable laws and regulations or the interpretation of such laws and regulations. There can be no assurance that we will be able to (or decide to) obtain any such licenses, certifications, and approvals. In addition, there are substantial costs and potential product changes involved in maintaining and renewing such licenses, certifications, and approvals, and we could be subject to fines or other enforcement action if we are found to violate disclosure, reporting, anti-money laundering, capitalization, corporate governance, or other requirements of such licenses. These factors could impose substantial additional costs, involve considerable delay to the development or provision of our products or services, require significant and costly operational changes, or prevent us from providing our products or services in a given market.

In many countries, it may not be clear whether we are required to be licensed as a payment services provider, bank, financial institution, or otherwise. In such markets, we may rely on local banks to process payments and conduct foreign exchange transactions in local currency. Local regulators may use their power to slow or halt payments to local merchants conducted through local banks or otherwise prohibit or impede us from doing business in a jurisdiction. Such regulatory actions or the need to obtain licenses, certifications, or other regulatory approvals could impose substantial costs, involve considerable delay to the provision or development of our services, require significant and costly operational changes, impose restrictions, limitations, or additional requirements on our business, or prevent us from providing any products or services in a given market.

Consumer Protection

We are subject to consumer protection laws and regulations in the countries in which we operate. In the U.S., we are subject to federal and state consumer protection laws and regulations applicable to our activities, including the Electronic Fund Transfer Act (“EFTA”) and Regulation E as implemented by the Consumer Financial Protection Bureau (“CFPB”). These regulations require us to provide advance disclosure of changes to our services, follow specified error resolution procedures, and reimburse consumers for losses from certain transactions not authorized by the consumer, among other requirements. Additionally, technical violations of consumer protection laws could result in the assessment of actual damages or statutory damages or penalties of up to $1,000 in individual cases or up to $500,000 per violation in any class action and treble damages in some instances; we could also be liable for plaintiffs’ attorneys’ fees in such cases. We are subject to, and have paid amounts in settlement of, lawsuits containing allegations that our business violated the EFTA and Regulation E or otherwise advance claims for relief relating to our business practices (e.g., that we improperly held consumer funds or otherwise improperly limited consumer accounts).

In October 2016, the CFPB issued a final rule on prepaid accounts. The rule’s definition of prepaid account includes certain accounts that are capable of being loaded with funds and whose primary function is to conduct transactions with multiple, unaffiliated merchants, at ATMs and/or for person-to-person transfers, including certain digital wallets. The rule’s requirements include: the disclosure of fees and other information to the consumer prior to the creation of a prepaid account; the extension of Regulation E liability limits and error-resolution requirements to all prepaid accounts; the application of Regulation Z credit card requirements to prepaid accounts with overdraft and credit features; and the submission of prepaid account agreements to the CFPB and their publication to the general public. In April 2017, the CFPB delayed the effective date of the final rule on prepaid accounts to April 1, 2018, and indicated that it would review, among other issues, the linking of credit cards to digital wallets that are capable of storing funds. In June 2017, the CFPB released proposed changes to its final rule, and in January 2018, the CFPB issued its final rule, modifying some aspects of the rule, with an overall effective date of April 1, 2019. We are in the process of implementing certain changes to comply with the final rule. We expect that such implementation will require us to make substantial changes to the design of certain U.S. consumer accounts and their operability, which could lead to customer dissatisfaction, require us to reallocate resources, and increase our costs, which could negatively affect our business.

In May 2015, we entered into a Stipulated Final Judgment and Consent Order ("Consent Order") with the CFPB in which we settled regulatory claims arising from PayPal Credit practices between 2011 and 2015. The Consent Order included obligations on PayPal to pay $15 million in redress to consumers and a $10 million civil monetary penalty, and required PayPal to make various changes to PayPal Credit disclosures and related business practices. We continue to cooperate and engage with the CFPB and work to ensure compliance with the Consent Order, which may result in us incurring additional costs.

PayPal (Europe) principally offers its services in EU countries through a "passport" notification process through the Luxembourg regulator to regulators in other EU member states pursuant to EU regulations. Regulators in these countries could notify PayPal (Europe) of local 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 or the PayPal group's activities in the local country directly or through a branch office. These or similar actions by these regulators could increase the cost of, or delay, our plans to expand our business in EU countries.

Table of Contents

Economic and Trade Sanctions

We are required to comply with U.S. economic and trade sanctions administered by OFAC and the Council of the European Union, respectively. We have self-reported to OFAC certain transactions that were inadvertently processed but subsequently identified as possible violations of U.S. economic and trade sanctions. In March 2015, we reached a settlement with OFAC regarding possible violations arising from our sanctions compliance practices between 2009 and 2013, prior to the implementation of our real-time transaction scanning program. Subsequently, we have self-reported additional transactions as possible violations, and we have received new subpoenas from OFAC seeking additional information about certain of these transactions. Such self-reported transactions could result in claims or actions against us, including litigation, injunctions, damage awards, fines or penalties, or require us to change our business practices in a manner that could result in a material loss, require significant management time, result in the diversion of significant operational resources, or otherwise harm our business.

Anti-Money Laundering and Counter-Terrorist Financing

We are subject to various anti-money laundering and counter-terrorist financing laws and regulations around the world that prohibit, among other things, our involvement in transferring the proceeds of criminal activities. Regulators in the U.S. and other regulators globally continue to increase their scrutiny of compliance with these obligations, which may require us to further revise or expand our compliance program, including the procedures we use to verify the identity of our customers and to monitor international and domestic transactions. Many countries in which we operate also have anti-money laundering and counter-terrorist financing laws and regulations, and we have been and will continue to be required to make changes to our compliance program in various jurisdictions in response. Regulators regularly re-examine the transaction volume thresholds at which we must obtain and keep applicable records or verify identities of customers and any change in such thresholds could result in greater costs for compliance. In the EU, the implementation of the Fourth Anti-Money Laundering Directive and the regulation on information accompanying transfer of funds (commonly known as the Revised Wire Transfer Regulation) may make compliance more costly and operationally difficult to manage, lead to increased friction for customers, and result in a decrease in business. Penalties for non-compliance with the Fourth Anti-Money Laundering Directive could include fines of up to 10% of PayPal (Europe)’s total annual turnover. On April 19, 2018, the European Parliament adopted the European Commission’s proposal for a Fifth Anti-Money Laundering Directive, containing more stringent provisions in certain areas, which may also increase compliance costs.

Privacy and Protection of User Data

We are subject to a number of laws, rules, directives, and regulations (which we refer to as “privacy laws”) relating to the collection, use, retention, security, processing, and transfer (which we refer to as “process”) of personally identifiable information about our customers and employees (which we refer to as “personal data”) in the countries where we operate. Our business relies on the processing of data in many jurisdictions and the movement of data across national borders. As a result, much of the personal data that we process, especially financial information, is regulated by multiple privacy laws and, in some cases, the privacy laws of multiple jurisdictions. In many cases, these laws apply not only to third-party transactions, but also to transfers of information between or among us, our subsidiaries, and other parties with which we have commercial relationships.

Regulatory scrutiny of privacy, data protection, and the collection, storage, use, and sharing of personal data is increasing around the world. There is uncertainty associated with the legal and regulatory environment relating to privacy and data protection laws, which continue to develop in ways we cannot predict, including with respect to evolving technologies such as cloud computing and blockchain technology.

Any failure, or perceived failure, by us to comply with our privacy policies and communicated to users prior to our collection, use, storage and transfer, and disclosure of their personal data, with applicable industry data protection or security standards, with any applicable regulatory requirements or orders, or with privacy, data protection, information security, or consumer protection-related laws and regulations in one or more jurisdictions could result in proceedings or actions against us by data protection authorities (which we refer to as "supervisory authorities"), governmental entities or others, including class action privacy litigation in certain jurisdictions, would subject us to significant awards, fines, penalties, judgments, and negative publicity arising from any financial or non-financial damages suffered by any individuals. This could, individually or in the aggregate, materially harm our business. Specifically, this would likely require us to change our business practices, and would increase the costs and complexity of compliance. In addition, compliance with inconsistent privacy laws may restrict our ability to provide products and services to our customers.

Table of Contents

PayPal relies on a variety of compliance methods to transfer personal data of EU citizens to the U.S., including reliance on Binding Corporate Rules ("BCRs") for internal transfers of certain types of personal data and Standard Contractual Clauses ("SCCs") as approved by the European Commission for transfers to and from third parties. PayPal must also ensure that third parties processing personal data of PayPal's EU customers and/or employees outside of the EU have compliant transfer mechanisms. In October 2015, the European Court of Justice invalidated U.S.-EU Safe Harbor framework clauses that were previously relied upon by some PayPal vendors to lawfully transfer personal data of EU citizens to U.S. companies, and PayPal entered into SCCs with those third parties who had previously relied on the U.S.-EU Safe Harbor framework. In July 2016, the U.S. and EU authorities agreed on a replacement for Safe Harbor known as "Privacy Shield." Both the Privacy Shield framework and SCCs are facing legal challenges in the European justice system. To the extent that the Privacy Shield or SCCs are invalidated, PayPal's ability to process EU personal data with third parties outside of the EU could be jeopardized.

In 2016, the EU adopted the General Data Protection Regulation ("GDPR"), which became effective in May 2018. The EU data protection regime expands the scope of the EU data protection law to all foreign companies processing personal data of EU residents, imposes a strict data protection compliance regime with severe penalties of up to the greater of 4% of worldwide turnover or €20 million, and includes new rights such as the "portability" of personal data. Although the GDPR applies across the EU without a need for local implementing legislation, each EU member state has the ability to interpret the GDPR opening clauses, which permit region-specific data protection legislation and have the potential to create inconsistencies on a country-by-country basis. Implementation of the GDPR has required us to change our business practices and increased the costs and complexity of compliance.

PayPal also faces additional potential challenges from local data protection agencies ("DPAs"). Because PayPal (Europe) is headquartered in Luxembourg and subject to regulation as a bank in that jurisdiction, we have relied on the "one-stop-shop" concept under which Luxembourg has been our lead data protection regulator in the EU. However, a 2015 European Court of Justice ruling (Weltimmo) affecting companies that do business in the EU potentially could make us subject to the local data protection laws or regulatory enforcement activities of the various EU member states in which we have established legal entities and which apply privacy laws that are different than, and may conflict with, Luxembourg privacy laws.

In addition, because of the large number of text messages, emails, phone calls, and other communications we send or make to our customers for various business purposes, communication-related privacy laws that provide a specified monetary damage award or fine for each violation could result in particularly significant damage awards or fines. For example, under the Telephone Consumer Protection Act ("TCPA"), in the U.S., plaintiffs may seek actual monetary loss or statutory damages of $500 per violation, whichever is greater, and courts may triple the damage award for willful or knowing violations. We have been, and may continue to be subject to lawsuits (including class-action lawsuits) containing allegations that our business violated the TCPA. These lawsuits seek damages (including statutory damages) and injunctive relief, among other remedies. Given the large number of communications we send to our customers, a determination that there have been violations of 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.

If one or more of our counterparty financial institutions default on their financial or performance obligations to us or fail, we may incur significant losses.

We have significant amounts of cash, cash equivalents, and other investments on deposit or in accounts with banks or other financial institutions in the U.S. and abroad. As part of our currency hedging activities, we enter into transactions involving derivative financial instruments with various financial institutions. Certain banks and financial institutions are also lenders under our credit facilities. We regularly monitor our exposure to counterparty credit risk, and actively manage this exposure to mitigate the associated risk. Despite these efforts, we may be exposed to the risk of default by, or deteriorating operating results or financial condition or failure of, these counterparty financial

institutions. The risk of counterparty default, deterioration, or failure may be heightened during economic downturns and periods of uncertainty in the financial markets. If one of our counterparties were to become insolvent or file for bankruptcy, our ability to recover losses incurred as a result of default or to access or recover our assets that are deposited or held in accounts with such counterparty may be limited by the counterparty's liquidity or the applicable laws governing the insolvency or bankruptcy proceedings. In the event of default or failure of one or more of our counterparties, we could incur significant losses, which could negatively impact our results of operations and financial condition.

Table of Contents

PayPal is not a bank or licensed lender in the U.S. and relies upon third parties to make loans and provide other products critical to our business, which raises additional risks.

As PayPal is neither a chartered financial institution, nor licensed to make loans in any state in the U.S., we rely on third-party chartered financial institutions to provide PayPal branded credit products to our customers in the U.S., including consumer credits products such as PayPal Credit and PayPal branded Mastercard credit cards, and business credit products such as PayPal Working Capital and PayPal Business Loan products. Any termination or interruption in a partner bank's ability or willingness to lend could interrupt, potentially materially, our ability to offer consumer and business loan products, which could materially and adversely affect our business. In the event of a partner bank's inability or unwillingness to lend, we may need to reach a similar agreement