Trust

This section describes our performance in and commitments to intellectual property rights protection, cybersecurity and data protection. A common thread weaving these priorities together is the pivotal importance of trust – from merchants, consumers, partners and regulators.

Intellectual Property Rights Protection

The protection of intellectual property rights (IPR) is core to the operation of a healthy marketplace. Trust is essential for the health and sustainability of Alibaba's business, and consumers and merchants place tremendous trust in our online marketplaces. We have established an industry-leading IPR operation that ensures we are a source of branded, authorized goods, and that strongly deters the sale of illicit or unauthorized goods, in order to protect the interests of rights holders, brands and consumers.

Intellectual Property Rights Protection

We are proactive in our approach, aiming to identify problems early before we receive complaints. Our IP Protection Department is charged with the critical responsibility of maintaining a healthy and dynamic business environment throughout Alibaba's e-commerce ecosystem.

This unit is led by our Chief Risk Officer, who is also our Chief Platform Governance Officer, and she reports directly to our CEO. Over 300 professionals work in this business unit including senior global team members who communicate with global rights holders and brand associations on a regular basis.

To effectively protect the rights of brand owners on our large online platform, we make extensive use of cutting edge, proprietary technology. Our proactive monitoring and takedown system for problematic listings is driven by sophisticated data-base algorithms and textual analysis and photo, optical character and behavior recognition technologies. Our philosophy is to partner with brands, understand their particular product characteristics, and utilize our technology to proactively monitor our platforms. Then, we make it easy for brands to report and track complaints – which over time has allowed us to continually improve our IP Protection Program.

Brands and brand owners are key constituents of our platform. We proactively established the Alibaba Anti-Counterfeiting Alliance ("AACA" or the "Alliance") in January 2017. AACA's 105 brand members include Adidas, P&G, Mars, Adobe, Danone, Hasbro, Samsung, and L'Oreal. With their support, the Alliance is effectively using internet technology and data to combat IP infringement more efficiently and transparently. We recently launched a program of IP Protection Roadshows in countries around the world where we present to global brands about the tools Alibaba offers to fight IP infringement. Additionally, we have a scheme to support small brands who may not have the same level of resources to protect their original designs or patents.

Working with brands is not enough. We also take the fight offline to work with trade associations, governments and law enforcement agencies in the fight to protect IPR. Industry groups we work with come from the automotive, digital content, apparel, electronics, luxury goods, food, pharmaceutical, and personal care sectors. We also partner with law enforcement agencies to provide leads of suspected illicit manufacturing facilities. We believe it's equally important to attack the bad actors at the source in the physical world. The goal is to encourage all parties to collaboratively fight counterfeiting through communication and information exchange.

We openly communicate our IPR efforts to the public by publishing an **Intellectual Property Rights Protection Annual Report** and **Intellectual Property Rights Protection Handbook**. We regularly report our progress in this program; our results speak for themselves.

Intellectual Property Rights Protection *continued*

PORTAL FOR PROACTIVELY RESOLVING IP PROTECTION ISSUES

We have a one-stop portal with authorized access for brands (**https://ipp.alibabagroup.com**) to manage our Notice and Take-down ("NTD") processes. The portal allow brands to track the status of their complaints and review sellers' appeals. Following new procedures launched in mid-2017, 95% of takedown requests were processed within 24 hours which represented a 68% reduction in processing time. In many cases, offending Taobao stores are simply shut down by us.

Results 2017

↑ 17%
Increase in the number of registered accounts in our IP protection system

↓ 42%
Decrease in takedown requests

240,000
Number of Taobao stores closed due to bad merchant behavior

24-hour takedown

95%
Takedown requests were processed within 24 hours*

68%
Representing a reduction in processing time**

* From June 2017 to December 2017
** Average processing time compared to 2016

Intellectual Property Rights Protection *continued*

Proactive takedowns enabled by technology (2017)

27X

More listings proactively removed than reactively taken down in response to requests from rights holders

97%

Number of all proactive takedowns removed before a single sale occured

PROACTIVE MONITORING TECHNOLOGY

We use state of the art technology to partner with brands to understand their specific product characteristics and, using our sophisticated algorithms and robust data processing and analytics technology, we detect, identify, block and remove suspicious product listings from our platform and penalize bad actors.

In 2017, Alibaba's real-time information scanning capabilities enabled the company to proactively remove vastly more listings than those flagged by rights holders. All but a few of these listings were eliminated before a single sale took place.

"The most powerful weapon against counterfeiting today is data and analytics, and the only way we can win this war is to unite. With our robust data technologies, we are confident the Alliance will accelerate the digital transformation in our global fight against counterfeits."

JESSIE ZHENG
Chief Risk Officer and Chief Platform Governance Officer, Alibaba Partner

Intellectual Property Rights Protection *continued*

HOW WE ENGAGE WITH BRANDS

The **Alibaba Anti-Counterfeiting Alliance** ("AACA") fosters transparency and communication among stakeholders and provides a forum for coordinating offline investigations and referrals to law enforcement. Here is a small selection of the 105 brands who are our members and allies.

This alliance focuses on:

- Building up brand and product-related knowledge for proactive monitoring
- Test buy programs for rapid enforcement
- Educating the public and launching campaigns to raise awareness among consumers
- Increasing quality of leads provided to law enforcement
- Taking problem merchants to court
- Sharing best practice and industry experience with relevant stakeholders

Intellectual Property Rights Protection *continued*

Law enforcement crackdowns (2017)

1,910

Number of leads provided to the police

1,606

Number of arrests made based on Alibaba referrals

1,328

Number of illicit locations closed down by law enforcement

¥4.3 BN

Total estimated value of goods involved

UNPRECEDENTED SUCCESS SUPPORTING LAW ENFORCEMENT

Our online portal and our technology tools both generate leads, complaints and data evidence about IP infringers' actions. Based on the information we collect and our ongoing engagement with brands, we approach and assist law enforcement officials in offline criminal and civil investigations.

In 2017, Alibaba supported local police in 23 provinces and cities throughout China in their efforts to crack down on the sale of counterfeit or otherwise inferior quality goods, leading to the arrest of more than 1,600 suspects and the closure of more than 1,300 facilities.

WINNING LAWSUITS AND TAKING BAD ACTORS TO COURT

In conjunction with the public appeal for stricter enforcement of IP laws in China, Alibaba was the first platform operator in China to bring civil lawsuits against merchants who misuse its services for the sale of counterfeit goods.

Intellectual Property Rights Protection *continued*

Case study

SWAROVSKI

In January 2017, Alibaba Group sued two vendors selling fake Swarovski watches via Taobao. This was the first-ever instance of an e-commerce platform taking a counterfeiter to court in China, sending a strong warning to illegal vendors and demonstrating our determination to fight fake products. The international brand Swarovski said in a statement that it is committed to protecting its brand and consumers from fraudulent selling activity, and it lauded Alibaba's efforts to protect brands and its platforms' integrity.

Case study

Mars Inc.

In July 2017, after investigating and collecting evidence in cooperation with Mars Inc. (a global producer of confectionary, pet food, and other food products), Alibaba won a landmark civil lawsuit in China against a seller infringing upon Mars Inc.'s products. A Shanghai court found the vendor guilty and ordered the defendant to pay damages. The case is believed to be the first of its kind in China, where an e-commerce platform has successfully sought compensation from one of its online retailers.

"We adopt a zero-tolerance attitude toward counterfeiting, and firmly preserve the rights and interests of consumers, as well as brand's reputation. Mars is determined to work with Alibaba and other parties to keep the market order, and build a healthy and lively market environment with all efforts. We look forward to continuing to working with Alibaba and others to dismantle the supply chain of counterfeit goods, and to create an environment where counterfeiters can no longer hide."

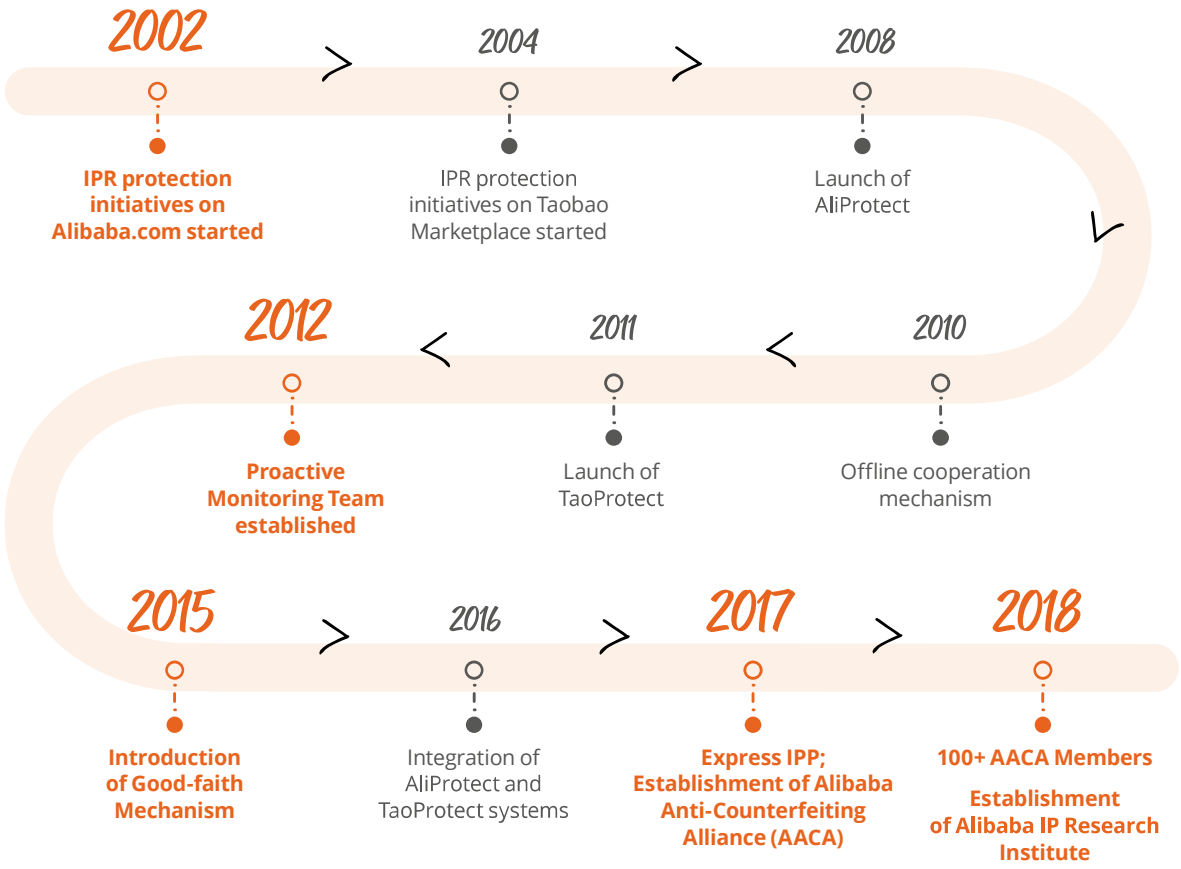
SCOTT THOMPSON
General Counsel of Marketing Properties at Mars Inc.

Intellectual Property Rights Protection *continued*

THE EVOLUTION OF IP PROTECTION IN ALIBABA

Milestones

- Email-based Notice Submission
- Online System & Proactive Monitoring
- Online to Offline Anti-Counterfeiting
- Multi-party Cooperation
- AACA



Cybersecurity

Security and accuracy of all the e-commerce transactions completed on our platforms are mission critical to consumers who spend money and to merchants whose business depend on making sales on our platforms. Because security is mission critical to our customers, we must treat it as our utmost priority.

Cybersecurity *continued*

We have developed industry-leading cybersecurity technology and practices that safeguard our e-commerce platforms. We recognize that consumers and merchants rely on us to protect their data on our platforms to ensure business sustainability.

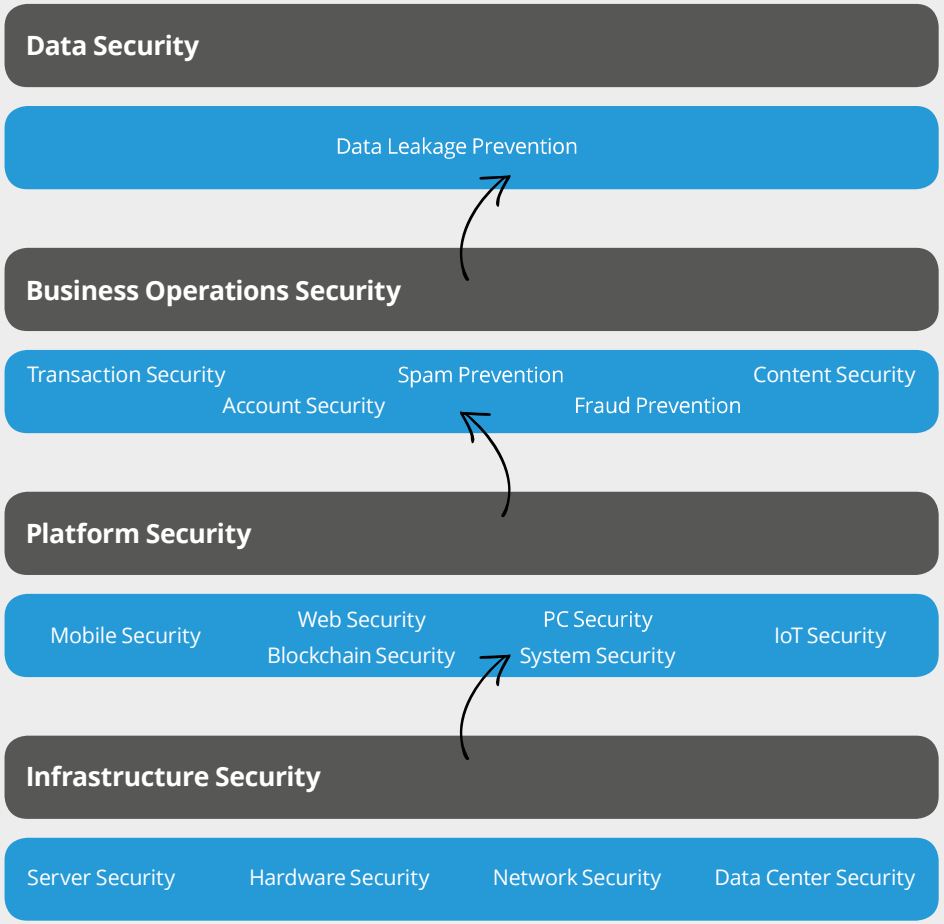
We also run the leading cloud computing service in China that many other businesses depend on to safely store data and process transactions, and our network security must be designed to withstand attempted intrusions.

We invest heavily and strategically in proprietary systems, cutting-edge technology, and R&D to build and safeguard a secure and protected environment across all our business units, in related companies and with ecosystem partners. Our multi-layer security system provides a comprehensive data security infrastructure for continuous monitoring and system protection throughout all platforms.

Our Chief Risk Officer (CRO), supported by our Chief Technology Officer (CTO), is responsible for cybersecurity. Both the CRO and CTO directly report to our CEO. Our CRO oversees the integrity of our IT system, ensuring that our systems are sound and well-defended. Our cybersecurity teams, who report to the CRO, focus on security standards, processes and breach avoidance. We also have a Cybersecurity and Data Protection Committee chaired by the CRO that oversees data security issues for all platforms and products across the Group.

On a continual basis, our CRO's cybersecurity team provides a comprehensive framework of compliance training, risk assessment and security testing to the CTO and other teams across our platform. The CRO team also provides continuous monitoring of potential breaches or incidents, including before an incident (through risk assessment), during an incident (through intrusion interception), and after an incident (with source tracking of data breach). We also place security teams in each functional department to help implement Alibaba's security strategy and manage daily security issues.

Multi-layer security system



Cybersecurity *continued*

EVIDENCE OF OUR BUSINESS SECURITY AND CYBERSECURITY CAPABILITIES

- Our real time risk management engine can do 30 billion protective scans per day at peak.
- Our remote personal authentication system for merchants is based on biometric identification.
- Our emergency management system responds to emerging data crisis situations. It ranks incidents and situations by levels of potential damage, so we can evaluate the scope of impact and assess the resources required to respond immediately.
- Our security systems have the capacity and resources to protect ourselves. We successfully defended the largest known DDoS attack to date in March 2018, which hit our platforms at a peak volume of 776Gbps.
- We are constantly improving our intrusion detection and prevention capability. We have a professional "red alert" team that simulates realistic external cyber attacks, in order to stress test our abilities to block intrusions.
- By deploying Security Development Lifecycle (SDL) to all the applications, we are continually reducing the number of vulnerabilities to improve application security quality.
- The cybersecurity team offers a "bug bounty" program to incentivize individual security developers to report bugs in our system.
- In order to continually prepare for security challenges in the future, we operate several R&D labs dedicated to researching innovative and pioneering security technologies, as well as Internet of Things (IoT) and blockchain.

Certificates and Standards

Alibaba follows best practice international standards. We meet ISO 27001 international certification standards, the global benchmark for information security management systems. Alibaba Group is certified by international standards* for data security and privacy measures, including:

- ISO27001 for information security management system
- ISO22301 for business continuity systems to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents
- Payment Card Industry Data Security Standard (PCI DSS)
- Report on System and Organization Controls SOC 1 and 2 by AICPA for data security, confidentiality and data privacy

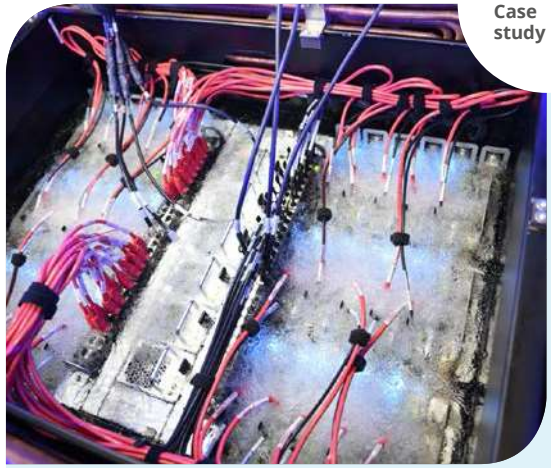
Furthermore, Alibaba Cloud is the first cloud services provider to be certified with the ISO27001 Information Security Management System Certification and to receive the CSA STAR Certification in China. Cainiao Network is the first logistics provider to be issued with the industry SOCII report.

* **Source:** China's Certification and Accreditation Unified Business Information Search Platform http://cx.cnca.cn/; International Standards Organization https://www.iso.org/standards.html; https://www.alibabacloud.com/trust-center

Cybersecurity *continued*

"Operating such a massive e-commerce platform, how do we guard against risks like malicious attacks, hackers, and fraud? Of course, we cannot take a case-by-case approach. We have to aggregate large numbers of logins or events to monitor security. We are continuously training our systems on the huge volumes of data we handle, and the system is becoming increasingly intelligent. We are the world-leading use case for artificial intelligence – and that is our advantage."

JESSIE ZHENG
Chief Risk Officer, Alibaba Partner



Case study

2017 11.11 Global Shopping Festival, a real testimony to our security capability

During the 2017 11.11 Global Shopping Festival, the total amount of paid transactions was RMB168.2 billion (US$25.3 billion) with 90% of the transactions executed via mobile devices. The Shopping Festival marked the biggest online shopping day in the world and was the most important marketing, promotion and sale event of the year for participating merchants – the smooth working of the transaction platform was mission-critical for our customers.

In order to protect consumers and merchants from cyber-attacks and fraudulent transactions, our cybersecurity team put in place robust security measures to filter out malicious activities and IP addresses to ensure transaction validity. On that day, the systems of Alibaba and our affiliate Ant Financial successfully processed peak orders of 325,000 per second, and 256,000 peak payment transactions per second, and our logistics subsidiary Cainiao managed 812 million total delivery orders.

325,000

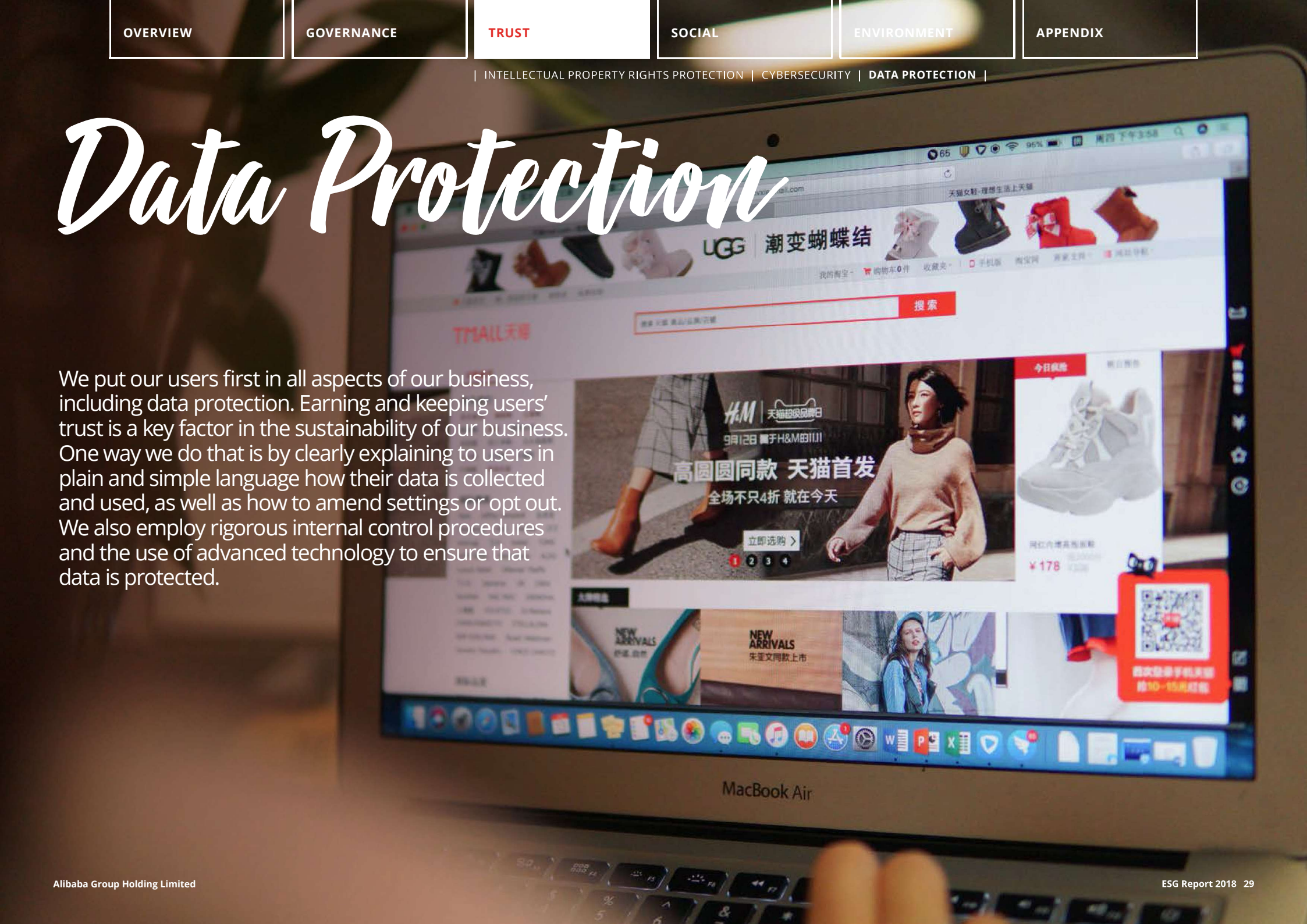
Peak orders successfully processed per second

256,000

Peak payment transactions per second

Data Protection

We put our users first in all aspects of our business, including data protection. Earning and keeping users' trust is a key factor in the sustainability of our business. One way we do that is by clearly explaining to users in plain and simple language how their data is collected and used, as well as how to amend settings or opt out. We also employ rigorous internal control procedures and the use of advanced technology to ensure that data is protected.



Data Protection *continued*

Data handling protocols are centralized and organized to ensure accountability; we enforce stringent guidelines and rules. We collect, classify and manage data in a rigorous and systematic manner to protect user privacy.

Data must be used for agreed objectives or purposes, in a relevant way, and within an agreed scope. Analysis of personally identifiable data is done on an aggregated, anonymized basis. We are committed to best practices such as limiting access to data only to designated personnel and minimizing data collection and retention. Operation logs are kept, and disaster recovery and backup mechanisms have been established to help guarantee data integrity.

We follow clear standards for sharing data among affiliates and related third parties, and we provide a self-developed secure data upload tool for affiliates and authorized third parties to access desensitized customer data.

We comply with applicable laws and regulations in the markets where we operate when sharing personal data of our customers with third parties, and we obtain opt-in or opt-out consents as required. In 2018, we have been devoting considerable resources to complying with the European Union's General Data Protection Regulation (GDPR).

Our Chief Risk Officer oversees both cybersecurity and data protection. We have a large team dedicated to developing our data protection policies and procedures, and we are engaged with data privacy experts worldwide, constantly learning from leading industry practices.

DATA CLASSIFICATION, ACCESS, AND USAGE

At the heart of how we manage data is the way we classify it. We have a detailed protocol for categorizing data along a spectrum of usage as well as sensitivity. We designate sensitive data as either customer's personally identifiable data, business data generated from our platforms, or Alibaba corporate data. Then we further classify data and assign security levels appropriately, into either public (level 1), internal (level 2), confidential (level 3), or secret (level 4- the highest).

The use of all data requires identity verification of the user applying for data access as well as authorization by designated responsible persons, and authorization is subject to time limits.

Differing levels of sensitive data are protected appropriately, so as to guarantee the safety of data use by our employees. For example:

- For massive data usage scenarios, it is mandatory for our staff to use our proprietary data leakage prevention tool to ensure data cannot be downloaded to the local hosts.
- We have robust measures, including proprietary mobile device management (Alilang) and data leakage prevention (Cloud Shell) software, which can prevent data leakage by monitoring abnormal behavior of employees and giving timely alerts to their managers.
- We are continually improving our data flow tracing capability, such as traceable watermarks embedded in company files.
- For our open platform, we encrypt level-3 and level-4 data before transfering to our authorized sellers' independent software vendors.

Alibaba Group and our affiliates, such as Ant Financial Services and our logistics subsidiary Cainiao Network, have a well-established framework in place to share certain types of data in controlled environments in order to improve our service offering to customers. We have implemented strict rules and protocols for data sharing with affiliates, including physical storage, prohibition of data duplication and a data oversight committee.

More information on policies regarding our Data Sharing Agreement with affiliates can be found in our most recent annual report on Form 20-F, page 201.

Data Protection *continued*

"Alibaba Cloud, our cloud computing arm, is a founding member of the EU Cloud Code of Conduct and the General Assembly, which helped to develop a code of conduct for EU cloud services in accordance with the requirements of the EU's General Data Protection Regulation."

ORGANIZATIONAL ACCOUNTABILITY

We have established three levels of organizational accountability for data collection and classification – at the group management level, business group level, and business unit level.

- At group management level, we have a Data Security Committee that is responsible for our official Data Security Guidelines around production, processing, transmission, storage, use, dissemination, and destruction of data, during all stages of the data life cycle.
- At the business group level, the President of each group is held accountable for data security, and each business unit has a dedicated expert who oversees data security issues.
- Each business unit formulates corresponding implementation rules, based on the Guidelines, which must be pre-approved and filed with the Data Security Committee.
- We also conduct training to improve the data security awareness of Alibaba employees and enforce compliance with our guidelines. Employees who are handling sensitive data are closely monitored to help avoid possible risks or losses resulting from improper data handling.

Employees are required to go through an annual data handling and protocol certification to ensure knowledge and sensitivity to our data policies. Any employees who violate the Data Security Guidelines are subject to penalty including dismissal, and we may also pursue civil and criminal charges against them.

COMPLIANCE WITH EVOLVING REGULATIONS

Alibaba is committed to compliance with government regulations in every jurisdiction in which we operate, and especially when the government orders enforcements or investigations. Separately, we have established procedures to support litigation, court orders, discovery and other legal matters that may require data disclosure but at the same time strictly minimize unnecessary disclosure of personal data.

In recent years, the European Union (EU), China, and other countries have strengthened the protection of private information of individuals and businesses, which we view as positive developments. We follow new PRC cyber security laws governing the collection of personally identifiable information (PII) and we are ISO27018 certified for measures that protect PII in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.