E-COMMERCE LEGAL GUIDE

New Markets Lab
In partnership with the Center for International Private Enterprise

May 2018
# E-Commerce Legal Guide

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviations and Acronyms</td>
<td>2</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Chapter I Regulation of Electronic Transactions</td>
<td>12</td>
</tr>
<tr>
<td>I.1 Electronic Payments</td>
<td>12</td>
</tr>
<tr>
<td>Regulatory Approaches to E-Payments</td>
<td>12</td>
</tr>
<tr>
<td>Implementation and Enforcement of E-Payments</td>
<td>17</td>
</tr>
<tr>
<td>Institutional Framework Related to E-Payments</td>
<td>18</td>
</tr>
<tr>
<td>International Framework for E-Payments</td>
<td>19</td>
</tr>
<tr>
<td>Key Takeaways for E-payments</td>
<td>20</td>
</tr>
<tr>
<td>I.2 Electronic Signatures</td>
<td>21</td>
</tr>
<tr>
<td>Regulatory Approaches to E-Signatures</td>
<td>21</td>
</tr>
<tr>
<td>Implementation and Enforcement of E-Signatures</td>
<td>24</td>
</tr>
<tr>
<td>Institutional Framework Related to E-Signatures</td>
<td>25</td>
</tr>
<tr>
<td>International Framework for E-Signatures</td>
<td>25</td>
</tr>
<tr>
<td>Key Takeaways for E-signatures</td>
<td>27</td>
</tr>
<tr>
<td>Chapter II Data Protection</td>
<td>28</td>
</tr>
<tr>
<td>Regulatory Approaches to Data Protection</td>
<td>28</td>
</tr>
<tr>
<td>Implementation and Enforcement of Data Protection</td>
<td>35</td>
</tr>
<tr>
<td>Institutional Framework Related to Data Protection</td>
<td>36</td>
</tr>
<tr>
<td>International Framework for Data Protection</td>
<td>37</td>
</tr>
<tr>
<td>Key Takeaways for Data Protection</td>
<td>39</td>
</tr>
<tr>
<td>Chapter III Cybersecurity</td>
<td>41</td>
</tr>
<tr>
<td>Regulatory Approaches to Cybersecurity</td>
<td>41</td>
</tr>
<tr>
<td>Implementation and Enforcement of Cybersecurity</td>
<td>46</td>
</tr>
<tr>
<td>Institutional Framework Related to Cybersecurity</td>
<td>48</td>
</tr>
<tr>
<td>International Framework for Cybersecurity</td>
<td>49</td>
</tr>
<tr>
<td>Key Takeaways for Cybersecurity</td>
<td>50</td>
</tr>
<tr>
<td>Chapter IV Consumer Protection</td>
<td>52</td>
</tr>
<tr>
<td>Regulatory Approaches to Consumer Protection</td>
<td>52</td>
</tr>
<tr>
<td>Implementation and Enforcement of Consumer Protection</td>
<td>57</td>
</tr>
<tr>
<td>Institutional Framework Related to Consumer Protection</td>
<td>57</td>
</tr>
<tr>
<td>International Framework for Consumer Protection</td>
<td>58</td>
</tr>
<tr>
<td>Key Takeaways for Consumer Protection</td>
<td>60</td>
</tr>
</tbody>
</table>
## Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH</td>
<td>Automated Clearing House</td>
</tr>
<tr>
<td>AfCFTA</td>
<td>African Continental Free Trade Area</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>APEC CBPRs</td>
<td>Asia-Pacific Economic Cooperation Cross-Border Privacy Rules</td>
</tr>
<tr>
<td>ASAPCP</td>
<td>Strategic Action Plan for Consumer Protection</td>
</tr>
<tr>
<td>ASEAN</td>
<td>Association of Southeast Asian Nations</td>
</tr>
<tr>
<td>CA</td>
<td>Certifying Authority</td>
</tr>
<tr>
<td>CAUCA</td>
<td>Unified Central American Customs Code</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CERT-MU</td>
<td>Computer Emergency Response Team of Mauritius</td>
</tr>
<tr>
<td>CIPE</td>
<td>Center for International Private Enterprise</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CPC</td>
<td>Consumer Protection Cooperation</td>
</tr>
<tr>
<td>CPTPP</td>
<td>Comprehensive and Progressive Agreement for Trans-Pacific Partnership</td>
</tr>
<tr>
<td>CSF</td>
<td>Cybersecurity Framework</td>
</tr>
<tr>
<td>DFS</td>
<td>Department of Financial Services</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officers</td>
</tr>
<tr>
<td>ECC-Net</td>
<td>European Consumer Centers Network</td>
</tr>
<tr>
<td>E-document</td>
<td>Electronic Document</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Network and Information Security</td>
</tr>
<tr>
<td>E-payment</td>
<td>Electronic Payment</td>
</tr>
<tr>
<td>E-signature</td>
<td>Electronic Signature</td>
</tr>
<tr>
<td>eIDAS</td>
<td>Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market</td>
</tr>
<tr>
<td>FTC</td>
<td>Federal Trade Commission</td>
</tr>
<tr>
<td>GLBA</td>
<td>Federal Gramm-Leach-Bliley Act</td>
</tr>
<tr>
<td>ICPEN</td>
<td>International Consumer Protection and Enforcement Network</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>MERCOSUR</td>
<td>Southern Common Market</td>
</tr>
<tr>
<td>MPIW</td>
<td>Mobile Payments Industry Workgroup</td>
</tr>
<tr>
<td>MSMRs</td>
<td>Micro, Small, or Medium Retailers</td>
</tr>
<tr>
<td>NAFTA</td>
<td>North America Free Trade Agreement</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute for Standards and Technology</td>
</tr>
<tr>
<td>NML</td>
<td>New Markets Lab</td>
</tr>
<tr>
<td>OAS</td>
<td>Organization of American States</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>ODR</td>
<td>Online Dispute Settlement</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Co-operation</td>
</tr>
<tr>
<td>OSCE</td>
<td>Organization for Security and Co-operation in Europe</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PSD2</td>
<td>European Union Directive on Payments</td>
</tr>
<tr>
<td>SMEs</td>
<td>Small- and Medium-Sized Enterprises</td>
</tr>
<tr>
<td>TSP</td>
<td>Trust Service Provider</td>
</tr>
<tr>
<td>UGC</td>
<td>User-Generated Content</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UNCITRAL</td>
<td>United Nations Commission on International Trade Law</td>
</tr>
<tr>
<td>UNGCP</td>
<td>United Nations Guideline for Consumer Protection</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
</tbody>
</table>
Executive Summary

As the world economy shifts further into the digital sphere, the nature of global commerce continues to change. Electronic commerce (e-commerce) traditionally referred to the buying and selling of goods and services online and has begun to include a new range of business opportunities that stand to disrupt existing industries. Digitally traded goods and services, digital content, and data analytics are fast becoming globally traded commodities. E-commerce is not only giving rise to new goods and services, it also provides a channel for engaging a broader range of businesses, including small and medium enterprises (SMEs) and women entrepreneurs, in international trade.

Even though SMEs and women are beginning to trade more internationally\(^1\) (for example, women account for nearly half of active online store owners in Alibaba’s retail segment\(^2\)), numerous legal and regulatory issues remain that may hinder the success of these businesses. The legal and regulatory framework for global e-commerce is quickly being outpaced by market innovation, and many countries do not yet have a legal system for e-commerce in place. Further, while legal and regulatory frameworks for e-commerce are evolving at the national – and sometimes sub-national – levels, there is not a set of harmonized international rules, giving rise to questions around cross-border e-commerce. As the e-commerce sector grows, companies, governments, and consumers will all have a direct stake in how rules and regulations for e-commerce are designed and implemented, and it will be particularly important to ensure that the concerns of all stakeholders are balanced as the rules evolve.

This E-Commerce Legal Guide (Legal Guide) was created as a user-friendly tool that takes stock of global trends in e-commerce regulation, existing regulatory practices in different parts of the world, and cross-cutting lessons, viewed from the perspectives of different stakeholders. It is a collaboration between the Center for International Private Enterprise (CIPE), a non-profit affiliate of the United States (U.S.) Chamber of Commerce, and the New Markets Lab (NML), a law and development center, which houses comparative expertise in socially accountable economic legal and regulatory reform. The Legal Guide is designed to help businesses and consumers understand the nature of existing rules surrounding e-commerce, provide a foundation to advocate for stakeholder needs based on regulatory options and global best practices (especially since many developing countries still lack relevant e-commerce rules), spur competition and inclusive growth, and provide a shared language for much-needed multi-stakeholder dialogue.\(^3\)

---

3 It is helpful here to briefly note the difference between laws, regulations, and policy. Laws (or acts), which often must go through a parliamentary process, create a framework for governing the market and often relate to a particular sector or activity. Laws tend to be more general and create legally enforceable obligations. Regulations are created, often through administration action, to implement laws and tend to be both more detailed and also easier to change. Policy, which is the broadest category of
Although many regulatory issues affect e-commerce, the Legal Guide focuses on four priority areas: (1) electronic transactions, specifically, electronic payment (e-payment) and electronic signature (e-signature), (2) data protection, (3) cybersecurity, and (4) consumer protection. All four areas were also highlighted by private sector associations surveyed by CIPE as priorities for enterprises of all sizes, particularly SMEs. These regulatory issues impact every link of the e-commerce supply chain, from the organizational structure of a company pre-transaction (for example, appointment a data protection officer), to the completion of transaction (for example, the adoption of affordable e-payment services), to issues post-transaction (for example, consumers’ right to withdraw from a transaction).

The four priority areas covered in this Legal Guide are also particularly relevant to the global conversation surrounding e-commerce and can act as force multipliers for broader reform. All are also subject to regulations that impact both the business transaction cycle, particularly when companies engage in cross-border sales, and e-commerce systems overall, making them central to both business opportunity and government concern. There are, of course, additional issues that deserve greater focus in the context of engaging SMEs in e-commerce, such as trade facilitation, which will be more comprehensively covered in future legal tools. Additional tools may also explore issues related to e-commerce regulation from a country or regional perspective, which would offer more specific information to SMEs, women businesses, consumers, and regulatory counterparts.

By focusing on these issues from the perspective of SMEs and consumers, two sets of stakeholders who have not been as heavily engaged in the evolving global dialogue despite their strong interests in the outcome, this Legal Guide will help identify key intervention points to support the continued growth of SMEs within digital trade. In each chapter, the Legal Guide assesses business needs, regulatory priorities and tradeoffs, factors that will impact effective implementation and enforcement of rules, institutional frameworks, and international initiatives. While e-commerce presents many opportunities for SMEs, several hurdles exist as well, ranging from lack of awareness of relevant rules and standards (for example, rules on cybersecurity), financial constraints (for example, inability to build local data centers), and limited human resources (for example, inability to appoint dedicated data protection officers). Additional challenges arise as enterprises trade and become subject to overlapping layers of regulation both among and within nations. In many countries, e-commerce is regulated at the national level, although some sub-national entities regulate in this area as well (for example, U.S. states). At the international level, regulation of e-commerce is still very much under development, making this Legal Guide and further discussion on the role of SMEs in e-commerce particularly timely.

Within each of the priority areas, private sector and government priorities must be balanced:

- **Regulation of Electronic Transactions:** Just like traditional commerce, e-commerce is made up of transactions and agreements between actors along the supply chain. Multiple issues will arise, such as authenticating an agreement, receiving payment, and resolving measures, provides guidance to stakeholders and government officials on what objectives laws and regulations should seek to achieve but does not tend to be legally binding instruments on their own.
disputes when they arise (covered under consumer protection).

- **E-Payments**: For every business operating online, e-payments can be a considerable hurdle, particularly when operating across borders and financial systems. E-commerce service providers want assurance that payments will come through without delay, and governments must make sure that transactions protect those with less market power. As a result, e-payments tend to be heavily regulated across the globe, with several different approaches depending upon the type of e-payment system used. Common priorities for both the public and private sectors include prevention of fraud and compliance with banking requirements, and security issues at the transactional level. Governments must also prioritize institutional infrastructure that can investigate problems as they arise and enforce rules in the case of a violation.

- **E-Signatures**: Behind most e-payments are the contracts that create the transaction. Electronic contracting is fast becoming a substitute to handwritten contracts, and clear rules around e-signatures – which signal that an enforceable contract has been concluded – are needed. E-signature systems provide assurance that obligations on the part of both the buyer and seller are valid, legal, and enforceable. Different regulatory approaches include regulations that treat e-signatures and handwritten signatures the same (technology-neutral regulation), regulations that tie the validity of e-signatures to underlying authentication technology (two-tiered regulation), and regulations that prescribe a limited subset of e-signatures to be legal (prescriptive regulation).

- **Data Protection**: E-commerce has helped drive the production and international circulation of an unprecedented amount of data. Data Protection has traditionally been a national focus, due in part to the strong national security and surveillance concerns of governments and consumers’ concerns about privacy protection. Some jurisdictions comprehensively regulate data (usually through an overarching regulation), while others tend to regulate by sector. Many data protection regimes also take an incremental approach, weighing considerations like sensitivity of data, rights of those who submit data (data subjects), or capacity and impact upon stakeholders. Companies now also want to leverage the massive quantity of available data to provide innovative goods and services and, as highlighted in a recent CIPE publication, some could use robust data protection systems to boost brand reputation and build trust with consumers and users. Globally, common ground is emerging for how to treat the data lifecycle (collection and processing, storage, transfer, and disposal) as well as other cross-cutting issues (responses to data breach, jurisdictional application, and rights of data subjects), yet further attention to this topic is needed, particularly to safeguard the interests of smaller enterprises and consumers.

---

• **Cybersecurity:** Like data protection, cybersecurity is fast becoming a global concern. In recent years, attacks on computers and information networks, both public and private, have grown in scale and severity, negatively affecting governments, industry, and consumers. The regulatory framework for cybersecurity has evolved in three stages: cybercrime legislation at the national level, followed by standards and guidelines initiated by the private sector, and more recently, broader legislation that comprehensively regulates cybersecurity.

• **Consumer Protection:** Protecting consumers is more critical than ever in the digital economy, and consumer confidence in e-commerce is a prerequisite for their participation in online shopping. Yet, conventional consumer protection regimes may be inadequate to address e-commerce specific practices, such as advertising on social media, that are constantly evolving to accommodate changing consumer habits. Most governments do not know how best to regulate to provide this protection. Regulatory approaches tend to focus on how to balance rights and obligations among stakeholders (governments, industry, and consumers) and how to integrate e-commerce specific considerations into conventional consumer protection regimes.

Several overarching themes are notable. First, law and regulation can only work within an effective institutional framework, particularly in technical areas such as data protection and cybersecurity. Many countries are increasingly integrating functions (for example, rulemaking, capacity building, and enforcement) and establishing a central regulatory watchdog that can minimize regulatory gaps, ensure policy consistency, and streamline compliance obligations for enterprises. For issues that are present in both online and offline commerce, such as payment and consumer protection, most countries have maintained existing institutional frameworks, and some have founded special units or engaged new entities to meet specific challenges arising from e-commerce (for example, third-party certification agents for e-signature). While e-commerce is often regulated at the national level, many sub-national bodies (for example, U.S. states) issue rules, regulations, guidelines, and standards that are more detailed and broader in scope than national frameworks. Enterprises should carefully consider legal requirements that may be applicable to them at both levels.

Implementation and enforcement are also an ongoing challenge around the world. The biggest issues stem from capacity constraints within both the public and private sectors. Another significant challenge is caused by differences within and across regulatory systems. Domestically, businesses may need to comply with conflicting and confusing regulations and standards. Globally, there is not yet a common approach that harmonizes national initiatives and makes it easier for different e-commerce systems to work together. This lack of regulatory compatibility and interoperability between different standards and technologies can make it difficult to complete international e-payments, for example.

Notably, across the globe, some countries have not enacted relevant legal and regulatory frameworks to regulate e-commerce more generally or the four priority areas highlighted in this
paper more specifically (this is especially true for cybersecurity and data protection).\textsuperscript{5} Others have started regulating in different ways and at varying paces. Some developing countries that may not be leaders in conventional trade are making strides to create an enabling environment for e-commerce (sometimes ahead of developed countries), which could increase their share of digital trade and enable their economies to leapfrog or complement traditional development strategies through industrialization. Belarus, for example, has legalized cryptocurrency, which is viewed by some as a move that could catalyze the development and uptake of innovative e-payment solutions. In addition, countries sequence their regulations of the four priority areas differently, depending on their capacities, growth trajectories of different industries, and awareness. Regulators and enterprises could use this Legal Guide as a basis for deliberating the appropriate sequencing and content of the legal framework within the four priority areas.

Finally, regulatory approaches within any given economy should be based on specific political, social, and market conditions. For instance, in consumer protection, China’s focus on third-party platforms to monitor and supervise online vendors is keyed to the local market structure, whereby a small number of well-funded players dominate the retail segment. This approach, however, may be ineffective in markets with a large number of SMEs. The practices identified in the Legal Guide, notwithstanding the diversity and distinctiveness across individual economies, are intended to be a point of departure for public-private engagement, regulatory reform, capacity building, international cooperation, and donor interventions.

Table 1. Summary of Current E-Commerce Regulatory Regimes and Recommendations

<table>
<thead>
<tr>
<th>Current Status</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Regulation of Electronic Transactions</strong></td>
<td><strong>E-Payments:</strong></td>
</tr>
<tr>
<td>• Regulatory frameworks governing e-payments tend to follow the type of service: 1) <strong>bank-related e-payments</strong> are, like banks themselves, heavily regulated in almost all jurisdictions and subject to prevention and compliance, authentication of online transactions, investigation, and enforcement; and 2) <strong>non-bank related e-payments</strong> are often regulated either before market entry (ex-ante regulation, which tends to follow regulatory requirements for bank-related payments) or enforced once enterprises are operating in the market (ex-post regulation).</td>
<td>• Regulators and enterprises should concentrate on bringing more low-cost options to market (especially for cross-border transactions), which will particularly benefit SMEs that need to rely on third-party e-payment solutions. To that end, enterprises could work with regulators to establish “Regulatory Sandboxes” to test out their products without facing legal liability and could encourage the adoption of less restrictive, ex-post regulation whenever feasible.</td>
</tr>
<tr>
<td>• Implementation and enforcement can be challenging due to the complexity of financial regulations. Some countries have established a “Regulatory Sandbox” to allow companies to test products without fear of violating rules.</td>
<td>• Enterprises using bank-related payment solutions need to understand regulations applicable to banking institutions. Banks tend to be heavily regulated across the globe and are supervised by a wide range of regulators, all of which could pose significant compliance burdens. Enterprises developing non-bank related payment solutions could find themselves subject to different regulatory approaches depending upon the markets in which they operate.</td>
</tr>
</tbody>
</table>

• The institutional framework to enforce e-payments is typically spread across multiple agencies and follows the bank-related or non-bank related distinctions noted above. Responsibility is often allocated between national and sub-national entities.

• International frameworks related to e-payments tend to be general, and so far, national systems have not been harmonized at the regional or international levels.

• The ongoing WTO Trade in Services negotiations, which would further liberalize the financial services sector, could expand the reach of e-payment solutions and provide SMEs worldwide with more affordable e-payment options. SMEs will be able to reap significant benefits even if only a group of WTO Members have committed to further liberalization.

---

** Regulation of Electronic Transactions **

**E-Signature:**
- E-signatures are regulated depending upon how the signature is viewed: 1) a **technology-neutral approach** views all types of e-signatures and handwritten signatures as equal; 2) **two-tiered regulations** recognize the legality and validity of multiple types of electronic signatures but give higher evidentiary value to digital signatures authenticated by certain technologies; and 3) **prescriptive, technology-specific regulations** only recognize limited types of e-signatures.

- Implementation and enforcement challenges have arisen when public sector actors such as courts and regulatory bodies are resistant to the acceptance of e-signatures. Multi-stakeholder campaigns could help overcome this hurdle.

- The institutional framework to enforce electronic signatures varies depending upon which regulatory approach the country follows and could include third-party certification bodies.

Most international instruments that regulate electronic contracts and electronic signatures recognize the functional equivalence between them and aim to harmonize national laws.

**E-Signature:**
- Enterprises should understand the legality and validity of different e-signatures both in their domestic market and in the markets in which they trade.

- SMEs might be best served by technology-neutral laws that establish functional equivalence between e-signatures and handwritten signatures, which are the easiest to comply with.

- Enterprises should also pay attention to legal exceptions, whereby some e-signatures can be invalidated.

- At the international level, UNCITRAL model laws exist that, if widely adopted, could promote harmonization of a technology-neutral approach that would facilitate digital trade and better address the needs of SMEs.

---

**Data Protection**

- Data protection regimes tend to contain 1) obligations applicable to each link of the data lifecycle (collection and processing, storage, transfer, and disposal); and 2) cross-cutting obligations that apply to all links (responses to data breach, jurisdictional applicability, and rights of data subjects).

- Compliance with complex and overlapping data protection laws is challenging.

- Enterprises should understand the laws and regulations that are applicable to them, which will depend upon both the residence of the individuals whose data they possess and where the stages in the data lifecycle (collection, processing, storage, or transfer) take place. This means that an enterprise can be subject to regulations in multiple jurisdictions, since most national regulations are not harmonized internationally; enterprises may need to design tailored compliance strategies.
protection obligations can be burdensome and costly, especially for SMEs. Particularly cumbersome are requirements to appoint data protection officers, requirements to establish local data centers, and registration requirements.

- Institutionally, the global trend is to establish a single central regulator with broad responsibilities, even though some jurisdictions have continued to split regulatory roles by sectors or functions.

- Internationally, there are notable initiatives to enhance regulatory compatibility between regions. Also, trade agreements are emerging as a way to require regulators to balance international trade and data protection.

Regulatory approaches fall within three categories: 1) cybercrime legislation, which is present in most jurisdictions with varying degrees of coverage; 2) private-sector-led multi-stakeholder frameworks, which institutionalize private best practices; and 3) broader cybersecurity legislation that focuses on preventative aspects (strategic, organizational, and monitoring mechanisms) and reactive aspects (such as responses to security breaches).

- Implementation of cybersecurity rules is challenging for SMEs, which tend to underinvest due to limited knowledge of the gravity of cybersecurity risks, lack of sufficient resources, and lack of information regarding standards and how to adopt them.

- Legislation and regulation are only part of an effective institutional framework, which must also include technical expertise, capacity-building, and cooperation. Some jurisdictions have one central regulator to carry out all functions, while others have a de-centralized system. National regulators and subnational regulators may both exist.

- International frameworks tend to contain general requirements and center around capacity building and information sharing.

Regulators and enterprises should work together to determine the most appropriate regulatory framework and how to stage its adoption and implementation.

- Industry best practices can be shared through multi-stakeholder initiatives, clear implementation guidelines, and flexible adoption methods; these approaches could help enterprises gain more information on standards and prioritize ways in which to adopt best practices, both of which would be particularly helpful for SMEs with limited capacity and underinvestment in cybersecurity.

- Regulators could also create incentives for enterprises to adopt best practices (for example, SMEs can benefit from certifications that enhance consumer confidence).

- Establishing a single regulator to manage all institutional functions could facilitate compliance, streamline regulation, build capacity (in both the public and private sectors), and avoid challenges and costs due to overlapping regulations.
Regulatory approaches primarily focus on: 1) how governments, industry, and consumers share responsibility for consumer protection (which stakeholder is responsible for which actions) and 2) the balance between conventional consumer protection regimes and e-commerce specific regimes.

Regulations tend to cover consumer needs at each phase of a transaction: the pre-purchase phase (duties to disclose and advertising), payment phase (terms and conditions of transactions, transparent/secure payment, and data protection), and delivery/after-sale phase (dispute resolution and redress and the right to withdraw/cancel (cooling-off period).

Implementation and enforcement of consumer protection regimes is challenging, particularly in the cross-border context, and can be alleviated by close cooperation across jurisdictions.

Institutionally, many jurisdictions have established central regulators with broad oversight functions. While most jurisdictions have directly replicated their institutional framework for online consumer protection to mirror systems in the off-line world, some have created special units to meet challenges arising specifically from e-commerce.

International frameworks provide guidance but are very general.

Regulators, enterprises (particularly e-commerce platforms), and consumers should work together to allocate responsibilities among them, which could depend upon market conditions and how well court systems function.

A notable aspect of online consumer protection is the liability of e-commerce platforms; requiring e-commerce platforms to perform an extensive list of functions such as information verification and supervision of online vendors could be efficient in markets with high market concentration but could disadvantage new entrants and SMEs.

Enterprises should examine whether there are e-commerce specific business aspects that may not be covered by the existing regulatory regime for consumer protection (for example, advertising through social media) that should be specifically addressed.

Enterprises and consumers should identify feasible dispute resolution mechanisms since merchant-customer disputes routinely arise in the post-sale phase. Options include litigation (including through small claims courts), online dispute resolution provided by public and private actors, mediation, and arbitration.

Internationally, consumer protection in e-commerce has not received the focus it deserves. While several initiatives exist, they tend to be general in nature and do not provide sufficient guidance to enterprises, governments, or consumers. Going forward, this may be an area in which a model law could be helpful, as could greater integration with the other areas of law and regulation covered in this Legal Guide.
Chapter I Regulation of Electronic Transactions

Just like traditional commerce, e-commerce is made up of transactions and agreements between actors along the supply chain. Several issues will arise for enterprises and consumers alike, such as rules on authenticating agreements, receiving payments, and resolving disputes (covered in Chapter IV on consumer protection). This chapter discusses electronic payments (e-payments) and electronic signatures (e-signatures), both of which are crucial components of any transaction and can accelerate the transition from a paper-based to an electronic documentation system.

I.1 Electronic Payments

E-payments are an integral part of e-commerce and have become widely adopted in recent years thanks to technological innovation and the massive penetration of cell phones and smartphones throughout the world. Enterprises can be both users and creators of e-payment solutions. The World Bank found that small retailers – or micro, small, or medium retailers (MSMRs) – made US $34 trillion in payments in 2015, of which about US $15 trillion, or nearly half, were made through electronic payment systems. Access to banking services is a considerable hurdle for both SMEs and consumers using banking related e-payment systems. However, small retailers are concerned about the high cost and limited options of e-payment solutions, as well a lack of regulatory harmonization and compatibility between different e-payment systems. For creators of e-payment solutions, understanding the rules surrounding e-payments can help enterprises proactively prioritize their resources to prepare for the due diligence process; more efficiently bring a product to market; and improve the ongoing viability, sustainability, and growth potential of e-payment solutions that incorporate the needs of small enterprises. This chapter reviews common issues and requirements that enterprises should be aware of when developing e-payment services or adopting existing services – such as Automated Clearing House (ACH) payments, PayPal, Alipay, Venmo, and Google Wallet.

Regulatory Approaches to E-Payments

E-payments systems are regulated for many of the same reasons that traditional financial services are. Governments want to foster financial inclusion, protect consumers (who will often not have as much information as the service provider), and promote the business environment and investment more broadly. Enterprises, of course, will want to offer services to meet growing market demands in a way that is both flexible and dynamic.

E-payments can be regulated similar to traditional banking services or may sometimes fall outside of these more established regulatory structures. Regulation of e-payments tends to fit into two categories: traditional or bank-related e-payments and non-bank e-payments, with each

---

Overall, bank-related e-payments are heavily regulated across the globe, and regulatory elements (prevention and compliance, authentication of transactions, investigation, and enforcement) tend to be similar. In contrast, regulatory systems for non-bank e-payments often follow one of two approaches: an ex-ante approach that proactively extends strict banking regulations to non-bank e-payment systems, and a hands-off, or ex-post approach, more focused on enforcement with less restrictive conditions for market entry. The latter tends to better encourage dynamic growth in the industry, although it is possible that countries with a more hands-off regulatory approach will shift to more structured systems over time. Diagram 1 summarizes current regulatory approaches.

Diagram 1. E-payment Regulatory Approaches

Source: New Markets Lab (2018)

A. Bank-related Electronic Payments

For many merchants and consumers, access to the banking system is the first hurdle in both electronic and traditional commerce. According to the World Bank, in 2014 two billion adults lacked access to the banking system or were underserviced; 55 percent of these were women.9

Small retailers and their potential customers tend to face high banking fees; a lack of necessary paperwork to open bank accounts; indirect costs (such as traveling costs to get to a banking branch or an ATM); economic and labor informality; unmet gender, religious, or cultural needs; and financial illiteracy. All of these factors act as barriers for the underserviced to access banking related e-payments.

For enterprises offering bank-related e-payments, this type of e-payment is heavily regulated in many jurisdictions, similar to banking transactions (summarized in Box 1). Fintech companies must comply with a number of regulations, many of which were adopted after the 2008-2009 global financial crisis. The dauntingly complex web of financial regulations has even fueled brand-new businesses, collectively termed “regulatory technology” that use data analytics to assist enterprises with compliance.

**Box 1: Common Banking Regulations**

The legal and regulatory environment affecting bank intermediated finance is multilayered and sometimes complex. At least three major types of regulatory measures, arranged according to functional lines, regulate banking in most countries around the world today:

- **Systemic regulations (or macro-prudential regulations):** This category of regulation covers a range of measures designed to identify and mitigate risks to the stability of the financial system as a whole. Some examples are countercyclical capital buffers, dynamic provisioning rules, reserve requirements, and quantitative restrictions on borrowers such as loan-to-value and debt-to-income ratios.

- **Prudential regulations (or micro-prudential regulations):** This category of regulation covers measures concerned mainly with the stability of individual financial institutions. Examples of micro-prudential regulations include minimum capital requirements, capital adequacy ratios, solvency margin requirements, restrictions on credit concentration or portfolio allocation, and reporting and disclosure requirements.

- **Non-prudential regulations:** This category covers all other financial regulations which can be achieved regardless of the financial health of an institution or the integrity of the system. Some examples include:
  - **Consumer protection regulations,** such as transparency and truth-in-lending disclosure rules that allow consumers to make informed decisions; they also cover privacy matters and personal data protection
  - **Financial fraud and financial crime regulations,** which range from anti-money laundering and counter terrorist financing measures to those prohibiting abusive investment arrangements and other fraudulent action
  - **Tax-related regulations,** such as codes that govern financial transactions and finance sector profits; they also cover, among others, tax transparency matters and mechanisms for the exchange of tax information
  - **Trade and investment-related regulations,** which may include economic and trade sanctions, as well as rules on the participation of foreign equity, the establishment of branches, borrowing from

---


**Prevention and Compliance:** Enterprises should pay close attention to compliance requirements, which are present in most jurisdictions. Identifying and following these requirements can be
difficult because the requirements are numerous and are often imposed by different authorities. Some of the most common prevention and compliance measures are:

- **Licensing**: Card issuers, such as banks or financial institutions, need to obtain licenses to operate (this is true in many countries, including Australia\(^{14}\));

- **Due Diligence**: Financial institutions must provide periodic statements or other reporting to satisfy obligations such as anti-money laundering programs, counter-terrorism, and tax transparency\(^{15}\) (for example, the European Union (EU) has set out some of these requirements in the Anti-Money Laundering Directive\(^{16}\)); and

- **Consumer Protection**: This is particularly important given common information asymmetry in financial services (consumer protection is covered more broadly in Chapter IV), and countries and card networks have enacted laws to safeguard different aspects of consumer protection in e-payment that cover the following three aspects:
  
  a) Disclosure of the cost, terms, and conditions of the transaction prior to the authorization of the transaction (for example, these requirements exist in Paraguay,\(^{17}\) Mexico,\(^{18}\) and the EU\(^{19}\));
  
  b) Limitation on fees, including credit and debit card fees (for example, the EU has capped debit card fee at 0.2 percent of the value of a transaction and credit card fee at 0.3 percent of the value of a transaction\(^{20}\)); and
  
  c) Limitation on the financial responsibility of consumers for unauthorized charges, merchandise ordered but never received, goods and services not accepted by the customer, double charges and other incorrect charges in the transaction. (for example, these requirements are present in Colombia,\(^{21}\) Argentina,\(^{22}\) and Kenya\(^{23}\)).

**Authentication of Online Transactions**: Merchants have an obligation to provide a secure environment for transactions, and different regulatory systems apply a variety of authentication mechanisms. The EU’s authentication standards provide tiered levels of security.\(^{24}\) The most secure authentication method is called “strong customer authentication,” which demands that the banking institution verify the customer through several methods, such as verification of

---

\(^{14}\) National Consumer Credit Protection Act 2009 (National Credit Act).


\(^{17}\) Ley Nº 5476 de 2015 de Paraguay.

\(^{18}\) Circular 29/2008 publicada en el Diario Oficial de la Federación el 11 de julio de 2008.


\(^{21}\) Colombia Ley 1480 de 2011

\(^{22}\) Ley 25.065 de 1998 de Argentina.

\(^{23}\) Consumer Protection Act, No. 46 of 2012.

\(^{24}\) Definition of “Strong customer authentication” per Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2)
information only the user knows (elements of knowledge). In the US, the authentication standard is a private-sector initiative known as Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS, which has become a global industry standard, determines authentication requirements based on company size and has become an integral part of card network contracts with merchants. Meeting the PCI DSS could be a significant burden for SMEs looking to incorporate card payments as part of their business, due to its complexity and the costs associated with its implementation.

Investigation: In the event that a customer cancels a transaction or reports one as suspicious, banking institutions will investigate the transaction at issue. Most countries impose time limits for these investigations, including notification of the challenged transaction. In some cases, the card network will charge a processing fee and a chargeback fee if the merchant did not address the customer’s complaint in a timely manner, or if due diligence was not used when confirming the identity of the cardholder. These additional fees and procedures could be barriers for SMEs wishing to use cards as a means of payment.

Enforcement: Notably, many bank-related e-payment systems use private enforcement through industry self-regulation. For example, many major card companies apply PCI DSS, which imposes certain security requirements on merchants. Noncompliance can lead to sanctions by the card network, such as fines and termination of merchant accounts.

B. Non-Bank Electronic Payments

Unlike traditional bank-related or account-based e-payments, non-bank e-payments tend to be regulated differently across countries. Enterprises should understand the approach that governs their jurisdictions, and the type of legal regime will likely be a factor in determining where companies will set up operations. At one end of the spectrum is ex-ante regulation, whereby regulators proactively determine the requirements for entering and operating in the market through either case-by-case regulatory approval (usually by the same institutions that oversee the banking system) or broader regulation.

Within ex-ante regulation, which effectively controls who gets to enter the market, there are pros and cons to different approaches. Case-by-case approval could preserve regulatory flexibility for new technologies but may be burdensome for enterprises. In India, for example, the Reserve Bank of India must pre-approve any proposed novel payment systems. Enterprises looking to bring new e-payment options into the market must take into account potentially lengthy applications for authorization and the need to effectively familiarize regulators with new systems and technologies. Alternatively, broad regulation may make it easier to encourage stakeholder awareness and participation, but this type of approach tends to be a bit less flexible. The EU

---

27 IT Governance, The 12 Requirements of the PCI DSS. Web.
28 PSD2 para (71) and Chapter 6; Fair Credit Billing Act. 15 USC 160; Fair Credit Billing Act. 15 USC 160.
31 India Payment and Settlement Systems Act of 2007, Chapter III.
takes a broad ex-ante approach through the Directive on Payments (PSD2), which regulates all e-payments, including non-bank e-payments, through newly created categories of institutions: payment initiation services, account information services, and payment institutions. Key substantive requirements include authorization to operate, business organization controls, registration requirements, and security standards.

At the other end of the spectrum is ex-post regulation, whereby regulators choose to monitor new payments systems rather than promulgate additional rules on market entry and operation. This type of approach helps spur innovation and creativity because enterprises are not burdened with a concern that their technology will become invalid under the law.³² For instance, in the US, public-private partnerships have allowed regulators to monitor the e-payment industry through an industry group. The Federal Reserve Banks of Boston and Atlanta established the Mobile Payments Industry Workgroup (MPIW), a diverse industry group comprised of key stakeholders in the payments systems industry such as banking, technology, and retail.³³ Other countries have taken similar approaches, including Kenya’s mobile money transfer system M-PESA (See Box 2). In Belarus, the use of cryptocurrencies was legalized – including exchange services, initial coin offerings, mining operations, and smart contracts – through presidential Decree Nº 8 On the Development of the Digital Economy.³⁴ Notably, it monitors but does not regulate business activities relating to cryptocurrencies.³⁵

Box 2: The Regulation of M-PESA in Kenya


| Implementation and Enforcement of E-Payments |

For SMEs and consumers, access to banking service remains a considerable challenge, and bank-related e-payments may be subject to a range of regulatory requirements as noted above. Even though there is a growing presence of non-bank, alternative payment service providers, these

---


³³ Its members include: America Trusts & Savings Bank, Dubuque; AT&T; Bank of America; BetterBuyDesign; Citi; Conexus; CTIA; Dunkin Brands; First Data Corporation; Fiserv; Gemalto; Giesecke & Devrient; Global Payments, Inc.; Google; Microsoft; Merchant Advisory Group; NACHA, The Electronic Payments Association; PayPal; Samsung; and, Walmart, amongst others.


new service providers often must rely on technology and licenses to provide e-payment services, particularly for cross-border payments, which could be difficult to obtain.\footnote{Capgemini, \textit{Top 10 Trends in Payments 2017: What you need to know}. Web. 2017.}

Challenges exist for regulators as well, who must implement and enforce the complex set of financial regulations. To assist both enterprises and regulators, “Regulatory Sandboxes” have emerged as a solution to help new players comply with the complex web of financial regulations. The term ‘Regulatory Sandbox,’ coined in the United Kingdom (UK), refers to a legally safe space for businesses to test new products, services, business models, and delivery mechanisms without adverse legal repercussions, all subject to monitoring by regulators.\footnote{Financial Conduct Authority (FCA), \textit{Regulatory Sandbox}, Web. November 2015.} This allows products to reach the market that might otherwise never have been launched or even tested.\footnote{Capgemini, \textit{Top 10 Trends in Payments 2017: What you need to know}. Web. 2017.} Other benefits of these mechanisms include better access to finance and payment services that reach the market faster and at lower costs.\footnote{FCA, \textit{Regulatory Sandbox}, Web. November 2015.} The UK, Australia, Singapore, Hong Kong and the Netherlands have already implemented regulatory sandboxes to promote innovation in the e-payment industry.

\textit{Institutional Framework Related to E-Payments}

Laws surrounding e-payments are complex, and institutional frameworks can be equally multi-faceted. At the national level, many jurisdictions have a multi-agency structure. For example, in the US, six different agencies control consumer financial protection oversight of depository institutions – traditional or account-based payment services.\footnote{U.S. Department of the Treasury, \textit{A Financial System that Creates Economic Opportunities: Banks and Credit Unions}. Web. June 2017.} Three more agencies deal with non-depositary institutions, such as non-bank e-payment services.\footnote{U.S. Department of the Treasury, \textit{A Financial System that Creates Economic Opportunities: Banks and Credit Unions}. Web. June 2017.} A multi-agency structure puts heightened pressure on companies to monitor and comprehend sometimes conflicting regulations and guidelines. There is less of a burden on companies when regulators coordinate to issue consistent rules, make information accessible, and alert companies of regulatory updates through a wide range of channels, such as social media accounts or mailing lists.

Jurisdictions also allocate responsibilities between national and sub-national entities differently. Some places, such as the US, have delegated more responsibility at the sub-national level (in this case, the state level). For instance, non-bank payment providers must obtain a new Money Transmitter License in each state in which the provider plans to operate.\footnote{Each State has adopted laws regulating Money Transmitter Licenses, a comparative chart is available at: Thomas Brown, \textit{50-State Survey: Money Transmitter Licensing Requirements}. Web.} Diagram 2 illustrates the institutional framework governing e-payments in the US and demonstrates how many more institutions have oversight over banks versus fintech. In contrast, the EU allocates much of the financial supervision at the Union level, with the European Central Bank and the European Banking Authority overseeing most of the financial.supervisions.
Diagram 2. E-payment Institutional Framework in the United States

Source: New Markets Lab (2018)

International Framework for E-Payments

As domestic markets become increasingly connected at the international level through cross-border e-commerce, movement towards an international e-payment system or set of standards will become more pressing in order to facilitate viable, convenient, and affordable transactions. International e-payments hinge on the ability for different payment services systems to work together, which is difficult to achieve due to a lack of harmonization of regulations and different platforms.\(^43\) Currently, enterprises must contend with limited available options, such as credit card companies and global services such as PayPal. That said, several multilateral and regional frameworks exist or are under negotiation related to e-payments. They tend to contain general requirements and leave abundant room for regulators to tailor legislation to the local context, as is true in other sectors. These frameworks are summarized in Table 2.

---

\(^{43}\) August Pons, Mengzhen Wang, and Lauren Sillman, *Regulatory Burdens on MSMEs and E-Commerce in Lebanon.*
Table 2. International Framework for E-Payment

<table>
<thead>
<tr>
<th>Frameworks</th>
<th>Main provisions</th>
</tr>
</thead>
</table>
| WTO Trade in Services Agreement (under negotiation) | • Aims to further the liberalization of services in general, including financial services and thus, indirectly, e-payment systems when considered as financial services (and e-payment providers as service suppliers).<sup>44</sup>  
• Focuses on non-discrimination principles and market access. |
| World Bank’s Financial Inclusion Global Initiative (non-binding) | • Develops knowledge, technical tools and policy recommendations related to e-payments  
• Focuses particularly on pricing and incentives, use of data generated by an individual or firm’s payment activity, technological and process innovation, and intermediaries<sup>45</sup> |
| Directive of the European Parliament and Council on Payment Services in the Internal Market (PSD2) | • Regulates all e-payments, including non-bank e-payments, through newly created categories of institutions: payment initiation services, account information services, and payment institutions  
• Requires authorization to operate, business organization controls, registration requirements, and security standards<sup>46</sup> |
| North America Free Trade Agreement (NAFTA) (under renegotiation) | • Improves transparency and predictability in parties’ respective financial services regulatory procedures |
| Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (awaiting ratification) | • Obliges parties to avoid any unnecessary regulatory burden on electronic transactions and facilitates input by interested persons in the development of their national electronic transaction framework<sup>47</sup> |

Source: New Markets Lab (2018)

**Key Takeaways for E-payments**

E-payment has been an essential element of online transactions. However, high cost and limited options (especially for cross-border transactions) affect business profit margins, particularly because SMEs often need to rely on third-party e-payment solutions.

For enterprises that are seeking to bring e-payment services to market, the information included in this chapter will help streamline the due diligence process and ensure ongoing viability and growth. More specifically, enterprises developing bank-related payment solutions should


<sup>46</sup> “payment initiation service” defined as a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider;  
“account information service” defined as an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider;  
“payment institutions” defined as non-banking institutions that provide payment services

<sup>47</sup> CPTPP Chapter 14.
understand relevant regulations applicable to banking institutions, which tend to be heavily regulated across the globe. On the other hand, enterprises developing non-bank related payment solutions could find themselves under the purview of different regulatory systems and could factor the differences in regulatory systems into their business decisions (for example, incorporation). One approach, which is more common for non-bank financial services, involves monitoring instead of proactive regulation and could better enable new e-payment solutions. Even in jurisdictions where market entry is heavily regulated (ex-ante regulation), enterprises could work with regulators to establish “Regulatory Sandboxes” to test out their products without legal uncertainty.

The ongoing WTO Trade in Services negotiations, which would further liberalize the financial services sector, could expand the reach of e-payment solutions and provide SMEs worldwide with more affordable e-payment options. SMEs will be able to reap significant benefits even if only a group of WTO Members have committed to further liberalization.

### I.2 Electronic Signatures

Traditional handwritten signatures are an established part of contract law and are not usually the subject of new legal initiatives. However, with the rise of purely digital agreements, the concept of e-signatures poses unusual challenges. Notably, the validity of e-signatures is essential to the transition from a paper-based to an electronic documentation system.

In its simplest form, an electronic signature (e-signature) is a computer-based personal identity. Over the last few decades, e-signatures and associated security concerns have become increasingly complex, ranging from basic digital copies of a person’s handwritten signature to digital signatures that involve third-party certifiers.

Electronic documentation can also greatly accelerate and simplify customs procedures and expedite movement of goods at the border (a component of trade facilitation), thus removing a persistent logistical bottleneck. Efficient electronic processing at the border can be particularly beneficial to SMEs that may have limited capacity to manage regulatory documentation and, when trading on third-party platforms, would need to ensure timely delivery of goods to obtain good customer reviews and build trust.\(^48\) The expansion of e-commerce will depend in part upon when the different forms of e-signatures are recognized under the law.

**Regulatory Approaches to E-Signatures**

For electronic contracts, one of the most important questions is the type of e-signature used, as different e-signatures could be treated differently under the rules. There are three main types of e-signatures, and they vary in the level of security they provide:\(^49\)

---


1) Click-to-sign Signatures: These include tick boxes, e-squiggles, scanned images, and typed names;
2) Basic E-signatures: The signer applies their hand-signature hand to the document electronically and the document as a whole is protected with a cryptographic digital signature owned by a service provider organization that acts as a “witness” to the signing;
3) Digital Signatures: These are the most advanced and secure type of signature. They use a certificate-based digital ID issued by a Certification Authority (CA) or Trust Service Provider (TSP), that uniquely links the signature to the identity of the signer. Usually, Public Key Infrastructure (PKI), a means of authentication and access control over untrusted networks such as open telecommunications network or the Internet, is used to verify the integrity of the document.

Depending upon how these three types of e-signatures are treated, in terms of their validity, legality, and admissibility in court, three regulatory approaches exist: technology-neutral systems, two-tiered systems, and prescriptive systems. These three approaches are illustrated in Diagram 3 and elaborated below.

Diagram 3. E-signature Regulatory Approaches

Source: New Markets Lab (2018)

Technology-Neutral Systems: Otherwise referred to as minimalistic or permissive laws, technology-neutral_laws or regulations treat handwritten signatures and e-signatures equally,

---

50 Hongkong Post e-Cert, Concepts of PKI. Web.
52 Adobe, Adobe Sign - Digital Signature FAQs. Web.
regardless of the underlying technology. Examples of countries with technology-neutral laws or regulations include the US (at the federal level), Australia, New Zealand, and Canada. A more technology-neutral approach is the least burdensome for enterprises and could provide assurance that existing and old technologies are legally valid, encouraging parties to enter into e-contracts and promoting the diffusion of specific technologies and e-contracts.

Two-tiered Systems: Tiered systems accept the legality and enforceability of all e-signatures. In contrast to technology-neutral systems, tiered systems accord various degrees of legal weight to e-signatures, depending upon the security level provided by their authentication systems. These jurisdictions also tend to define specific types of digital signatures that respond to varying levels of security certification. Examples of frameworks with two-tier systems include the EU, most Latin American countries, and Russia.

Prescriptive Systems: This approach limits the scope of legally valid electronic signatures. Compared to the other two systems, the prescriptive system is the most restrictive and technology-specific. Some prescriptive systems not only deny rights that arise from an electronic transaction, but they may also impose legal sanctions when an e-signature falls outside of a specified list of legal e-signatures schemes. Examples of prescriptive systems include India, Malaysia, and several U.S. states. Prescribing the use of a specific technology or a specific electronic signature could create barriers for enterprises that are not aware of or are unable to adopt the underlying technology. This approach could also undermine the ability of enterprises to develop new types of signatures or adopt new technologies. For instance, South Korea’s prescriptive approach has resulted in enterprises maintaining outdated authentication systems.

International markets are also fragmented by these different approaches, and enterprises engaging in cross-border trade may have to consider multiple requirements in order to guarantee the validity of their contracts. Common regulatory elements exist and will be addressed below: 1) the recognition of electronic contracts and handwritten contracts as equal (functional equivalence) and the legality and enforceability of electronic signatures; 2) exceptions to valid e-signatures; and 3) definitions of different types of e-signatures.

First, most jurisdictions recognize the validity of electronic contracts, including their e-signatures. This is because the validity of contracts tends to depend upon the intent of the parties to be

---

54 Uniform Electronic Transactions Act (1999); Electronic Signatures in Global and National Commerce Act (2000)
58 OASIS PKI, Electronic Signature Laws and Regulations. Web.
59 The European Union’s Regulation N°910/2014.
60 DocuSign, eSignature Legality Guide. Web.
63 Information Technology Act 2000.
64 Digital Signature Act 1997.
65 Even though at the federal level the US is categorized as an open jurisdiction, each state has its own particular laws that can be classified as open, two-tier or prescriptive.
66 The case of South Korea and its financial transactions clearing technology is a good parallel of the effects outdated technologies can have. Scott J. Shackelford, Scott Russell, and Jeffrey Haut, *Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks*. Web. 2016.
bound by an agreement, regardless of whether the contract is in written, electronic, or verbal form (for example, Argentina,67 Australia,68 New Zealand,69 and Canada70 all recognize the validity of electronic contracts through legislation or regulation). In addition to confirming that e-contracts have the same status as traditional contracts, most jurisdictions now accept electronic signatures in the development of regular business and consider them enforceable in court. It is part of the parties’ burden of proof to demonstrate in court that the electronic signature presented is valid and has not been altered (for example, the laws in the EU,71 Colombia,72 Mexico,73 and the Philippines all uphold this burden of proof74).

Second, most jurisdictions also establish exceptions that explicitly invalidate certain categories of e-signatures. Enterprises operating in these jurisdictions should switch to use hand-written signatures in these cases. While countries differ in their specific lists of exceptions, common exceptions are focused around inheritance and family law issues such as divorce. For instance, the Czech Republic excludes certain instruments from e-signature, including those related to inheritance law, such as contracts, estate sales, and renunciation of succession rights, among others.75 Others also exclude specific legal processes, such as the granting of power of attorney in India and the exclusion of notarization in Brazil.76 In the U.S. state of California, judges have decided that even though digital signatures are appropriate in many business settings, they do not constitute an absolute replacement for original handwritten signatures.77

Additionally, for all two-tiered and prescriptive jurisdictions, it is important to define and distinguish between basic e-signatures and digital signatures. The difference between an electronic signature and a digital signature is that digital signatures are more secure and, therefore, are presumed as valid and legal in judicial proceedings.

**Implementation and Enforcement of E-Signatures**

Implementation and enforcement challenges have also arisen with respect to e-signatures, although, notably, the challenges tend to arise primarily from the public sector. For instance, in China, some judges are averse to recognizing e-signatures, despite the law’s clear recognition of them.78 In Sri Lanka, e-signatures were initially not given full weight following passage of the Electronic Transactions Act, but these issues were overcome through a multi-stakeholder campaign, which could be duplicated elsewhere (See Box 3).

---

67 Section 1017 of the Civil and Commercial Code.
71 The European Union’s Regulation Nº910/2014.
72 Electronic Signature has been recognized by law in Colombia since 1999, with the passage of Law 527 "Legal and evidential validity of data messages" and later regulated with regards to electronic signature by Decree 2364 of 2012.
73 Mexico has no uniform law on electronic signatures, rather, eSignature legality in Mexico is governed by multiple applicable laws and regulations set out by various legal bodies.
74 Electronic Signature has been recognized by law in the Philippines since 2000, with the passage of The Electronic Commerce Act.
75 Section 1582 (2) of the Civil Code), inheritance sales (Section 1714 (3) of the Civil Code), renunciation of succession right (Section 1484 of the Civil Code)
77 United States Bankruptcy Court Central District of California, New Local Bankruptcy Rule 9011-1, effective December 1, 2017
In 2006, Sri Lanka passed the Electronic Transactions Act. No. 19, which recognized the legality and validity of e-signatures; however, “bureaucratic resistance to change and administrative lethargy” impeded the implementation of the Act. Prompted by a multi-stakeholder campaign, the government issued central guidelines to catalyze the acceptance of e-signatures, which paved the way for Electronic Document (e-document) processing platforms and shorter customs procedures.


Institutional Framework Related to E-Signatures

The institutional framework surrounding e-signature depends upon whether the law gives special value to different technologies. Countries with flexible, and in some cases two-tiered systems, are technology-neutral jurisdictions. In technology-neutral jurisdictions, the institutional framework needed to enforce e-signatures is the same as traditional signatures: namely, courts and arbitral bodies that adjudicate contracts.

In contrast, many countries with technology-specific regulatory approaches (most prescriptive and two-tiered systems) have created a completely independent institutional framework for the enforcement and validation of digital signatures that includes government agencies and private actors. In such cases, some relationships and interactions are restricted by legal provisions, while others are tied completely to whatever contract terms each party has agreed to. In such cases, private actors can act as certifying bodies; these include CA or TSP discussed above, which are common in the EU and Argentina, for example. These regulated private actors must obtain licenses from governmental agencies and can provide certification services if they adhere to technological standards. For example, the EU’s regulation eIDAS establishes that TSPs shall be audited by a conformity assessment body to confirm the fulfillment of the legal requirements. In Argentina, a similar process is established with the addition of the technological standards, which a company must follow to become a CA.

International Framework for E-Signatures

Several multilateral and regional frameworks are applicable to e-signature. At the international level, most of the efforts have been led through the United National Commission on International Trade Law (UNCITRAL). As the core legal body of the United Nations system in international trade law, UNCITRAL has promoted harmonized and modern rules on commercial transactions through a range of initiatives, including model laws and rules with global acceptance.
Some regions, such as Latin America, have multiple frameworks that could eventually be consolidated, and enterprises in the region should watch developments in this area closely. These frameworks are summarized in Table 3 below.

Table 3. International Frameworks for E-Signatures

<table>
<thead>
<tr>
<th>Frameworks</th>
<th>Main provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multilateral</td>
<td></td>
</tr>
</tbody>
</table>
| UNCITRAL Model Law on Electronic Commerce\(^{83}\) | • Promotes functional equivalence between digital messages and handwritten ones, which amounts to legal recognition of electronic contracts.\(^{84}\)  
  • Recognizes electronic signatures as a way to sign electronic documents. \(^{85}\)  
  • Emphasizes equal evidentiary weight to digital messages than that given to handwritten documents. \(^{86}\) |
| UNCITRAL Model Law on Electronic Signatures | • Reflects technology-neutral approach: validity of all types of electronic signatures recognized, regardless of the technology they use\(^{87}\).  
  • Recognizes non-discrimination of foreign electronic signatures: (validity of an electronic signature instead hinges on technical reliability). \(^{88}\) |
| ALADI Digital Certificate of Origin\(^{89}\) | • Aims to obtain gradual harmonization and acceptance of forms of e-signatures\(^{90}\)                                                                 |
| Southern Common Market (MERCOSUR)\(^{91}\) | • Recognizes validity of electronic signatures within the MERCOSUR region\(^{92}\)                                                                   |
| Unified Central American Customs Code (CAUCA)\(^{93}\) | • Recognizes the use of electronic documents for customs purposes and the use of functional equivalence between electronic signatures and handwritten signatures.\(^{94}\) |
| Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) | • Establishes a tired system with three types of electronic signatures that are recognized throughout the EU: 1) a simple e-signature, 2) an advanced e-signature similar to a digital signature, and 3) a qualified e-signature that has the security of a digital signature and is approved by a supervising body\(^{95}\) |
| African Continental Free Trade Area (AfCFTA)\(^{96}\) | • Encompasses the use of electronic certificate of origin and electronic signatures throughout various customs processes.\(^{97}\) |

Source: New Markets Lab (2018)

---

\(^{83}\) However, these instruments are not binding, unless the signatory country decides to adopt them as such. UNCITRAL Secretariat confirms that so far 32 States have legislation based or influenced by the Model Law.

\(^{84}\) UNCITRAL, “Model Law on Electronic Commerce”. Articles 4 and 5

\(^{85}\) Model Law on Electronic Commerce. Article 7

\(^{86}\) Model Law on Electronic Commerce. Article 9

\(^{87}\) UNCITRAL Model Law on Electronic Signature. Article 2, 3, and 6.

\(^{88}\) UNCITRAL, Model Law on Electronic Signatures. Article 12; UNCITRAL, Guide to Enact the UNCITRAL Model Law on Electronic Signatures.

\(^{89}\) Argentina, Bolivia, Brasil, Chile, Cuba, Colombia, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay, and Venezuela

\(^{90}\) UNCTAD. Study on the harmonization of cyberlegislation in Latin America. 2015.

\(^{91}\) Argentina, Brazil, Uruguay and Paraguay

\(^{92}\) Resolution No. 37/06 and Resolution 3/06.

\(^{93}\) Costa Rica, Dominican Republic, El Salvador, Honduras, Guatemala and Panama have adopted the Unified Central American Customs Code.

\(^{94}\) UNCTAD, Study on the harmonization of cyberlegislation in Latin America. Web. 2015.

\(^{95}\) European Union’s Regulation Nº910/2014

\(^{96}\) Agreement signed by 44 African countries creating an African Continental Free Trade Area.

\(^{97}\) AfCFTA. Annex 2 Rules of Origin; Annex 3 Customs Co-Operation and Mutual Administrative Assistance; and Annex 4 Trade Facilitation. The AfCFTA was signed in March of 2018 and is still in the early stages of developing a full legal text and implementing provisions that do exist.
**Key Takeaways for E-signatures**

E-signatures play a significant role in electronic transactions and are an important issue as the transition from a paper-based to an electronic documentation system progresses, with implications for commercial contracts and logistical efficiency. SMEs, in particular, can profit from efficient electronic processing, given that they may have limited capacity to manage regulatory documentation such as customs procedures and need to ensure timely delivery of goods to receive good customer reviews and build trust.\(^9^8\)

To ensure that e-signatures are valid, enterprises should understand the rules regarding different types of e-signatures in the different markets in which they operate. For SMEs, technology-neutral regulations that establish functional equivalence between all e-signatures and handwritten signatures are the easiest to comply with. Enterprises should also pay attention to exceptions, whereby jurisdictions invalidate certain categories of e-signatures. At the international level, UNCITRAL model laws exist that, if widely adopted, could promote harmonization of a technology-neutral approach that would facilitate digital trade and better address the needs of SMEs.

Chapter II Data Protection

Characterized as the oil of the digital economy, data have become a key global commodity and are increasingly harnessed, processed, exchanged, and analyzed in massive quantities to power digitalized content, goods, and services. Data protection has thus become a focal point for enterprises, regulators, and consumers alike. All data follow a lifecycle – data collection and processing, storage, transfer, and disposal – which underpins most regulatory approaches around the globe. Regulation tends to follow the steps in the data lifecycle (collection and processing, storage, transfer, and disposal), and enterprises may have different obligations depending upon their business model. Regulations also often include cross-cutting obligations, such as responses to a data breach.

It will be crucial to determine the data protection regimes that may apply to businesses that collect, process, store, use, or transfer personal data. Obligations can be far-reaching. First, enterprises should understand data protection regimes in their jurisdictions. Second, they will need to track the country or countries of residence of the individuals whose personal data they possess and then evaluate whether the data protection laws of those countries apply to them. They may, for instance, be required to embed specific data protection systems in daily business operations or build local data centers to store data (the so-called data localization requirement). Compliance can be burdensome, especially for companies that rely on international data flows and must comply with multiple data protection regimes.

Enterprises should also be vigilant about regulatory developments around the world: a growing list of countries, such as Kenya, Brazil, and Nigeria, are in the process of drafting their first data protection laws.\(^9\) For governments, regulating data requires a delicate balance among several factors: national security, surveillance, competition policy, innovation, the integrity of electoral process (especially after the recent Cambridge Analytica incident), and consumer protection. Consumers are also worried about how their personal data will be collected and used, particularly in sensitive areas such as biometric data. For example, consumers may be concerned with advertisements for commercial or political purposes that have been targeted based on personal data.

Regulatory Approaches to Data Protection

While there is a broad consensus on the necessity of data protection, due to cultural and historical variations, countries differ in their perceptions of data protection. For some, such as the EU, data protection includes both data security and privacy. For others, such as China, data protection mostly refers to data security.\(^1\)


\(^1\) Center for Strategic and International Studies, *What the Facebook Scandal Means in a Land without Facebook: A Look at China’s Burgeoning Data Protection Regime*. Web. April 25, 2018
These varying approaches at the country level have translated into differences in the scope and focus of regulations:

- Some countries have adopted more comprehensive overarching regulations (for example, the EU, Japan, and Ghana), which broadly cover all activities that involve data under a single legal instrument.
- Others (for example, the US) tend to regulate sector-by-sector.\(^1\) For instance, in the US, the Health Insurance Portability and Accountability Act of 1996 covers medical information in the healthcare industry.
- Regulations may also distinguish based on sensitivity of data (for example, in the EU and Russia, more stringent requirements apply to sensitive data), the capacity and data impact of entities (for example, in Australia, with exceptions, businesses with an annual turnover of AU$3 million or less are not subject to the Privacy Act\(^2\)), or special categories of people (for example, children – the Child Rights Act No. 26 of 2003 in Nigeria protects the privacy of children under 18).
- Further, some jurisdictions are more consumer-centric. For example, the EU, through the General Data Protection Regulation (GDPR), grants more control and a range of rights to consumers, which will be discussed in more detail below.

In practice, data protection regimes can include a mix of policy instruments, such as constitutional provisions, laws, regulations (for example, the GDPR in the EU), and standards (for example, GB/T 35273-2017 Information Technology – Personal Information Security Specification in China).\(^3\) Regardless of the policy instruments, common regulatory elements include both obligations governing steps in the data lifecycle (collection and processing, storage, transfer, and disposal) and cross-cutting obligations (responses to a data breach, the application of domestic laws to overseas enterprises, and rights of individuals whom data are about). These regulatory elements are mapped in Diagram 5 below.

---


Diagram 5. Regulatory Elements of Data Protection Regimes

Source: New Markets Lab (2018)

Obligations Governing Different Stages of the Data Lifecycle

Collection and Processing: Companies that are collecting and processing data in the course of their business operations must have valid grounds for doing so, including the consent of those who hold the data. This is increasingly being spelled out in countries’ laws; for example, Egypt’s draft Data Protection Law introduced a consent requirement. Globally, consumer consent is regulated differently depending upon the jurisdiction. For instance, the EU’s GDPR has particularly detailed consent requirements, including a standalone request for data processing that is separate from other terms and conditions. In addition to consent, regulators may specify other grounds for data collection; for example, Russia allows for the collection of data related to the performance of a contract or for statistical or scientific purposes.

Storage: Many countries require that businesses store data on servers that are physically located within their national boundaries through so-called data localization requirements. Examples include Germany, Russia, Greece, China, Malaysia, and Australia. Regulators justify data localization in a variety of ways, such as the protection of domestic privacy against foreign countries with lower data protection standards, safeguarding against foreign espionage, and

---

creation of employment opportunities associated with building and operating data centers. Many enterprises, particularly those working in more than one country, report that data localization requirements are financially burdensome and can divert sometimes limited financial resources from more productive uses. For SMEs, these requirements can discourage business operations that rely upon international data flows. For instance, in 2013, on average, building data centers in Brazil and Chile were estimated to cost US $60.3 million and US $43 million, respectively. As will be discussed below, some international trade agreements now include provisions to curb this trend.

Data Transfer: Countries and sub-national bodies restrict cross-border data transfer to varying degrees. Transfers can be permitted under one-time exceptions or ongoing-exceptions. One-time exceptions (for example, for the fulfillment of contracts) are common. However, ongoing exceptions are treated very differently and generally require an assessment of whether there is a sufficient degree of protection for the transfer of personal data.

Ongoing data transfers are typically handled by data receiving countries under one of the following four approaches, with differing implications for companies and data exporting governments:

- Evaluation of whether the domestic laws of the data exporting country are adequate (adequacy approach);
- Assessment of whether the independent review mechanisms of a given enterprise are sufficient (binding rules approach; for example, EU Binding Corporate Rules (BCR) system and Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPRs);
- Evaluation based on contractual protections (model contracts approach; rarely used); or
- Assessment based on whether individuals have consented to the data transfer (consent approach).

From a strategic point of view, if an enterprise is based in a jurisdiction with weak data protection laws, it may prefer the binding rules approach. The model contracts approach would also be an option, but is used much less frequently (to date, it is used only in the EU) and depends upon full implementation of model contracts. On the other hand, if an enterprise is located in a jurisdiction with strong data protection rules, it could request that its government seek ‘adequacy status’ from another jurisdiction (such as the EU), which would streamline data transfer overall. The strengths and weaknesses of each approach are included in Table 4.

Disposal: Once data have fulfilled their intended purposes (for example, when a transaction is completed), some jurisdictions (for example, the US at the federal level, some states in the US,
and the EU\textsuperscript{111}) require their destruction or disposal of the data. In such jurisdictions, enterprises essentially would need to carefully track a wide range of hardware and software that they use for data storage to ensure complete disposal of all relevant data. Enterprises may also need to designate or hire records retention managers to ensure complete and secure disposal of data, especially for data that are stored in cloud services.\textsuperscript{112}

**Table 4. Different Approaches for Managing Cross-Border Data Transfer**

<table>
<thead>
<tr>
<th>Approach</th>
<th>Strengths</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adequacy</td>
<td>Enables comprehensive transfer (for those countries found adequate) Promotes interoperability and harmonization Transparent and open ‘whitelist’</td>
<td>Causes significant difficulty for those countries that are not found adequate Struggles to accommodate jurisdictions with different approaches to data protection Lengthy process to determine adequacy</td>
</tr>
<tr>
<td>Binding rules</td>
<td>Enables free movement of data within a corporate group Promotes best practice data protection processes and oversight in the private sector Transparent and open list of participating companies</td>
<td>Lengthy and expensive approval process Limited use for other data transfers outside the corporate group</td>
</tr>
<tr>
<td>Model contracts</td>
<td>Promotes interoperability and harmonization Can be quickly implemented by individual businesses willing to adopt the model contractual clauses verbatim</td>
<td>Challenging to develop appropriate model clauses and to keep them up to date No transparency about who is using model clauses Limited opportunity for oversight</td>
</tr>
<tr>
<td>Consent</td>
<td>Quick and easy solution for certain types of transactions No detailed analysis or review required Low compliance burden for businesses</td>
<td>Completely unsuitable for many contemporary transactions Open to differing interpretations of consent and prone to complaints and disputes Potential for lack of fairness in situations where there is a significant power imbalance between the parties Potential to promote fragmentation rather than harmonization of data protection practices</td>
</tr>
</tbody>
</table>


**Cross-cutting Regulatory Aspects Across the Data Lifecycle**

**Responses to Data Breach**

While data breaches are undesirable, they are also fairly common. In order to build a resilient system that can withstand and minimize the impact of data breaches, many jurisdictions have imposed obligations regarding risk management and incident response. Regulations tend to broadly cover organizational, monitoring, and incident response measures. At the organizational level, some countries, such as the EU and China, require the establishment or appointment of dedicated data protection officers (DPOs). More stringent requirements may apply to some organizations (for example, those whose core business revolves around the large-scale processing of sensitive personal data). In the EU, DPOs must possess "expert knowledge" of data protection law and practice.\textsuperscript{113} However, because of the short supply of experienced data protection professionals, some enterprises may need to outsource the DPO role to an external provider, which could result in substantial costs for SMEs.\textsuperscript{114}


Monitoring is critical to detecting potential data breaches early on. Some jurisdictions have adopted a risk-based approach, undertaking risk mitigation measures tailored to the level of exposure. These efforts are aimed at detecting vulnerabilities in the data lifecycle and enhancing the resilience of organizational data protection systems. Mexico, for instance, imposes obligations to carry out a security risk analysis.\textsuperscript{115}

Incident response encompasses the actions governments or enterprises will need to take in the event of a data breach. Some jurisdictions have mandated notification, including Mexico\textsuperscript{116} and all 50 U.S. states.\textsuperscript{117} The requirements vary in their specificity and coverage but generally include the following components: (1) who must comply with the law (for example, businesses or public entities), (2) coverage of the information, (3) definition of a data breach, (4) requirements for notice (for example, timing or method of notice), and (5) exemptions (for example, encrypted information).\textsuperscript{118} To ensure the practicality and effectiveness of incident response, China also requires organizations to put in place incident response plans and conduct emergency drills at least once a year.\textsuperscript{119}

Rights of Data Subjects

Data subjects are the individuals who possess the personal data in use. Governments sometimes step in to provide a range of rights for data subjects, such as consumers, who generally do not have sufficient bargaining power to shape company data protection policies. The EU’s user-centric approach to data, under which GDPR provides for a broad scope of rights from which regulators could draw, is a good example of a rights-based data regime. These rights, which range from the right to be informed to the right to rectify inaccuracies and erase personal data, are summarized in Diagram 6.\textsuperscript{120}

\textsuperscript{115} DLA Piper, Data Protection Laws of the World. Web.
\textsuperscript{116} Linklaters, Data Protected People's Republic of China. Web.
\textsuperscript{117} National Conference of State Legislatures, Security Breach Notification Laws. Web. March 29, 2018
\textsuperscript{118} National Conference of State Legislatures, Security Breach Notification Laws. Web. March 29, 2018
\textsuperscript{120} GDPR; Information Commissioner’s Office, Guide to the General Data Protection Regulation (GDPR). Web.
Some rights, in particular, could stimulate competition and support SMEs. For instance, China’s regime and a draft bill in Brazil have both embraced additional rights for data stakeholders.\textsuperscript{121} In these countries, data stakeholders can request that a copy of their data be directly transmitted from one controller to another (data portability). A smooth transmission of data, enabled by interoperability between different websites and platforms, could encourage new market entrants and increase competition in the service of potential clients who are otherwise unwilling to re-input all their data.\textsuperscript{122} It is important that rights are clear since ambiguous terms could complicate implementation or lead to overly broad application. For instance, the right to not be subject to automated decision-making, including profiling, could threaten the legal certainty of programs that detect fraud and cybercrimes.\textsuperscript{123}

**Jurisdictional Reach**

There is a growing trend for regulators to apply domestic laws to overseas e-commerce enterprises that engage with domestic residents (extra-territorial reach), which could further increase compliance cost for businesses.\textsuperscript{124} In Japan, the data protection law expressly applies to foreign entities that collect or have collected personal information of individuals residing

\textsuperscript{122} PricewaterhouseCoopers, GDPR-Data Portability. Web.
\textsuperscript{123} DLA Piper, Data Protection Laws of the World. Web.
in Japan.\(^{125}\) Similarly, the EU’s GDPR contains an extra-territoriality clause that covers a number of overseas companies, such as those that process personal data of EU residents. Enterprises should, therefore, have a clear sense of where the personal data that they possess originates and will need to balance the cost of compliance against access to consumers.

**Implementation and Enforcement of Data Protection**

Enforcing data protection is an ongoing challenge. Two particular aspects of enforcement – heavy sanctions and the right for private actors to claim compensation – are worth particular focus. For regulators contemplating heavy sanctions, it is important to recognize the potential drawbacks. For instance, breach of a data protection law could lead to revenue-based fines of up to four percent of annual global turnover in the EU and imprisonment for 6-12 months in Japan.\(^{126}\) While heavy sanctions could encourage companies to prioritize their resources to comply with data protection laws, they could also lead to forum shopping, thus negating the deterrence effect of heavy fines and disproportionately affecting SMEs. For instance, to reduce exposure to the stringent requirements under the EU’s GDPR, multinational companies such as LinkedIn and Facebook, through revised terms of service, will move the legal jurisdiction of one and half billion users from Ireland to California before the effective implementation date of the GDPR. In other cases, enforcement officials (for example, those in China) may themselves perceive the fines to be too hefty and consequently sidestep the fines in favor of less stringent alternatives such as administrative warnings.

The second noteworthy aspect of data protection enforcement is that some jurisdictions allow consumers to bring private claims. As a case in point, Ghana’s Data Protection Act expressly provides for the “Right to Seek Compensation through the Courts” as part of data subjects’ right.\(^{127}\) Likewise, the EU’s GDPR explicitly sets a low bar and provides multiple avenues for private actors to seek redress. The GDPR’s “non-material damage” clause (for example, non-monetary harms) is actionable against data controllers or processors and permits consumers to register complaints with law enforcement.

Overall, for companies, compliance with data protection regimes can be costly and cumbersome. A report by Organization for Economic Co-operation (OECD) highlighted that multinational companies spend over US $1 million in data-related compliance costs.\(^{128}\) For SMEs, keeping abreast of, comprehending, and complying with a mix of evolving global and national regulations can be especially cumbersome. Three requirements, routinely present in national regulatory frameworks, have been identified as particularly burdensome for small businesses: (a) requirements to appoint data protection officers, (b) data localization requirements, and (c) registration requirements.

Registration requirements can be a particular challenge for SMEs. The first type of registration requirement involves notifying local data protection authorities of relevant businesses or

---


For instance, in Ghana, data controllers and processors must provide notification to the Data Protection Commission of things such as the type of data the enterprise holds and the nature of processing that the enterprise undertakes. Registration fees can be substantial in some countries (750 Ghana Cedis or about US $167 in most cases in Ghana). Another type of registration is a membership-based scheme, such as those in Europe and APEC (European BCR and APEC CBPRs), which entails fees such as application payments to the scheme operator and third-party certification services for initial certification and annual recertification; this type of registration also takes quite a bit of time (an average of 18 months is required for obtaining the EU certification).

To lighten compliance burden for SMEs, regulations could be drafted to differentiate based on firm revenue or include other built-in exemptions (for example, Australia’s Privacy Act contains certain exceptions based on firm revenue). Regulatory commitments may also be applied incrementally based on capability (for example, longer grace periods can be applied for implementing certain obligations for enterprises under a certain size).

For governments, enforcing data protection can be challenging due to capacity constraints and lack of awareness. Awareness-building campaigns could help create incentives for businesses to comply and would be a much lower-cost alternative to enforcement actions. The enforcement challenge is highlighted by Commission on Human Rights and Administrative Justice in Ghana:

“Even though the Commission has received some complaints about data breaches, enforcement actions under the Act have not been actively enforced because of the need to create awareness and also to develop the mechanisms to effectively implement enforcement actions including criminal prosecutions... There is a need to create further awareness and to build capacity among stakeholders including prosecutors and judges in order to effectively enforce applicable sanctions under [Ghana’s Data Protection] Act.”

**Institutional Framework Related to Data Protection**

At the national level, many countries are trending towards establishing a single central regulator that has broad legislative and oversight responsibilities. This approach streamlines compliance obligations for enterprises, provides a single point of contact for consumers seeking information or redress, and helps drive a single set of standards to minimize domestic and global regulatory fragmentation. Examples include the Data Protection Supervisor in the EU (established in

---

2010), the Data Protection Commission in Ghana (established in 2012), as well as the Personal Information Protection Commission in Japan (established in 2016).

Other jurisdictions split regulatory roles by sectors or functions. In China, for instance, the Ministry of Industry and Information Technology and the Cyberspace Administration of China regulate data protection in the telecommunications and Internet sectors, while the People's Bank of China and China Banking Regulatory Commission supervise data protection in the banking and finance sectors. Further, South Korea divides regulatory and complaint management functions between two agencies.

Private actors play a key role in the enforcement of data protection laws. In the US, private litigation has considerably driven the development and enforcement of data protection regimes. In addition, third parties are becoming increasingly active in certifying compliance with various regulatory schemes.

**International Framework for Data Protection**

Discrepancies between national frameworks exist, making it difficult to understand the rules on data protection when operating in multiple markets. Companies that rely on data imports or exports may face increased compliance costs or an inability to operate in certain markets. International initiatives to harmonize national frameworks are underway but typically only set out general principles. Table 5 below summarizes the major global, regional, and bilateral instruments applicable to data protection.

Among these initiatives, the APEC Privacy Framework is notable for its potential to increase regional coordination, which could streamline compliance obligations for enterprises. The APEC Privacy Framework was created to promote a common set of data protection rules and standards to facilitate cross-border data transfer. It lays down a single framework of principles and implementation guidelines (for example, security safeguard) and allows its 27 members to adopt the Privacy Framework with flexibility. As introduced above, the APEC CBPRs is a voluntary, enforceable scheme under the Privacy Framework that certifies companies’ compliance with the Privacy Framework and provides legal certainty for cross-border data transfer. Employing CBPR as a baseline standard can be particularly helpful to SMEs whose businesses revolve around cross-border data transfer but do not have the resources to formulate their own privacy programs; this advantage is particularly pronounced in the Association of Southeast Asian Nations (ASEAN) economies, where SMEs comprise 96 percent of all businesses.

Further, the potential interaction between APEC CBPRs and the EU data transfer mechanisms is critical to reducing compliance costs for businesses targeting both APEC and the EU markets. Talks between APEC and the EU to develop a means to streamline the dual certifications (“the

---

Referential”) are well underway.  

While it is uncertain whether and when the dual certification program will be in place, obtaining APEC certification appears to expedite and lower the cost of certification under EU BCR and could be a consideration for companies that are considering future expansions into the EU market.  

For instance, a company with an APEC certification reported that its BCR approval was four months shorter than the average of 18 months because any disparity between APEC CBPR and EU CBR did not require much internal change.

Internationally, trade agreements are increasingly tightening the linkage between international trade and data protection. In contrast to privacy-specific initiatives, trade agreements do not impose significant positive obligations but call for a balance between data protection laws and trade considerations. This balancing was advocated by the US and is fast becoming the standard approach, as evidenced by the US-South Korea Free Trade Agreement, the CPTPP (the follow-on agreement to the Trans-Pacific Partnership), and the recently concluded Singapore-Sri Lanka Free Trade Agreement (text unavailable).  

The inclusion of data provisions within trade agreements could limit the degree to which nations will have the flexibility to address data protection and may require governments to simultaneously balance a broad range of policy areas, such as environmental protection and tariff reduction.

Table 5. International Framework for Data Protection

<table>
<thead>
<tr>
<th>Framework</th>
<th>Key Provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multilateral</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Convention for the Protection of Individuals Regarding Automatic Processing of Personal Data | • Enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected  
• Prohibits the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards  
• Restricts cross-border transfer of personal data to states that do not provide equivalent protection |
| OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data | • Provides eight privacy principles and concepts with broad international support (for example, risk assessment and improved interoperability) that have influenced many national laws |
| **Regional** | |
| CPTPP | • Requires the adoption and maintenance of a legal framework that provides for the protection of the personal information of the users of e-commerce  
• Restricts data localization, subject to at least three exceptions: government data, financial services, and a general (four-step test) exception  
• Restricts limitations on data transfer, subject to a general four-step test exception |

140 Center for International Governance Innovation, Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. Web. April 4, 2018
### APEC

- Establishes a set of principles and implementation guidelines (for example, security safeguard and limitation on the collection and use of data) to facilitate the transfer of data among APEC members
- Allows companies to obtain certification to demonstrate compliance with APEC Privacy Framework through a voluntary mechanism

### African Union Convention on Cyber-security and Personal Data Protection

- Aims to establish regional and national legal frameworks for data protection

### Economic Community of West African States (ECOWAS) Supplementary Act on Data Protection

- Prescribes the required content of data privacy laws
- Requires the establishment of a data protection authority

### North America Free Trade Agreement (NAFTA) (under renegotiation)

- Ensures that countries refrain from imposing measures in the financial services sector that restrict cross-border data flows or that require the use or installation of local computing facilities\(^1\)\(^{141}\)

#### Bilateral

### US-South Korea Free Trade Agreement

- Requires parties to “refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders” in non-binding terms

---

**Key Takeaways for Data Protection**

Countries around the world are increasingly recognizing the critical importance of data protection and are enacting data protection laws as a response. In particular, some countries with large numbers of Internet users (for example, Kenya, Brazil, and Egypt) are drafting bills to protect data; enterprises should engage in these discussions in order to ensure that their needs are addressed.

Enterprises should also consider steps that are necessary to comply with existing regimes and implement self-regulation to build strong brands (given increasing consumer focus on data protection). First, enterprises should understand the range of laws and regulations that are applicable to them. This will depend upon the residence of the individuals whose data they possess, the laws of their home jurisdiction, and the stages in the data lifecycle the activities of their enterprise fall under (collection, processing, storage, or transfer). Data protection laws are increasingly applied to overseas enterprises when they collect or process data of domestic residents, so this should be an area of increased focus for enterprises.

---

\(^1\)\(^{141}\) USTR, *Summary of Objectives for the NAFTA Renegotiation*. July 2017

---

*Source: New Markets Lab (2018)*

---

141 USTR, *Summary of Objectives for the NAFTA Renegotiation*. July 2017
Enterprises should also carefully examine the specific regulatory requirements that are applicable to their operations. Notably, enterprises whose business models center on cross-border data transfer should consider the approaches that could enable data transfer and evaluate them based on factors such as similarities between laws/regulations in two jurisdictions or contractual terms. They could also work with regulators to use international instruments to harmonize rules, provide for mutual recognition, or subscribe to private certification schemes such as APEC CBPRs.

Compliance with data protection regimes can be burdensome, especially for SMEs. To lighten the compliance burden, enterprises could take advantage of exemptions in areas such as requirements to appoint data protection officers, registration requirements (including fees), and data localization requirements.
Chapter III Cybersecurity

The growth of e-commerce and advancement of technology have widened enterprises’ market base in domestic and overseas markets, fueled job growth (particularly for women), and lowered barriers to entry compared to conventional trade.\(^{142}\) Meanwhile, Internet and technology have also given rise to a new area of international crime. For instance, in 2017, a data breach at Equifax, a major credit reporting agency, exposed the sensitive personal information of as many as 147.9 million consumers.\(^{143}\) Also in 2017, a global ransomware attack infected computers in 150 countries, affecting private companies such as international shipper FedEx and crippling public entities such as 16 hospitals in the UK.\(^{144}\) Critically, SMEs are particularly vulnerable to cyber attacks,\(^{145}\) so it is imperative to implement technical and organizational strategies to ensure cybersecurity. Cybersecurity is an increasingly common term which refers to the security of an enterprise’s assets (or user’s assets in the consumer’s case) in the cyber environment. Broadly, cybersecurity covers “connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information.”\(^{146}\) An important subset of assets is data, covered in Chapter II above.

**Regulatory Approaches to Cybersecurity**

Countries typically regulate through a combination of measures, which have evolved over time. The first wave of regulation focused on cybercrime legislation, which is a public-centered, top-down approach. The second phase involved private-centered, bottom-up approach regulation following the 2008 financial crisis. The third phase consists of the more comprehensive cybersecurity legislation that has become common in recent years. Diagram 7 portrays the three phases of regulations, which will be addressed in greater detail below, and enterprises may have compliance obligations across measures.

\(^{146}\) International Telecommunications Union, Definition of Cybersecurity. Web.
A. Cybercrime Legislation

A range of cybercrimes exist (See Diagram 8), and early cybersecurity legislation focuses mainly on this aspect. Enterprises should familiarize themselves with the common cybercrimes, report potential criminal activities, and seek redress. Regulators could familiarize themselves with the range of cybercrimes and consider benchmarking their national laws against the list.

Importantly, without sufficient sanctions and enforcement capacity, cybercrime legislation will not be fully effective. For instance, in 2012, Brazil passed its first cybercrime law, which is accompanied by light sanctions (such as house arrest) and enforced only by understaffed and underfunded cybercrime divisions.\textsuperscript{147} Despite the enactment of this law, in 2017, Brazil was still ranked as the country with the most victims of cybercrimes in Latin America, with malware and online fraud as the primary crimes.\textsuperscript{148}


### Diagram 8. Common Types of Cybercrimes

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail Spoofing</td>
<td>Manipulating commercial e-mail to falsely the email’s true origin, without the consent or authorization of the user whose email address is spoofed.</td>
</tr>
<tr>
<td>Phishing</td>
<td>The act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by tempting another’s identity in an official-looking email, IM, etc.</td>
</tr>
<tr>
<td>Spamming</td>
<td>Unlawful commercial advertisements sent by e-mail over the Internet. There’s legislation addressing spam in at least 33 countries, including the EU.</td>
</tr>
<tr>
<td>Cyber-Defamation</td>
<td>False and unprivileged statement of fact that is harmful to someone’s reputation and published “with bad,” meaning as a result of negligence or malice.</td>
</tr>
<tr>
<td>Cyberstalking</td>
<td>Using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person.</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>Wrongfully obtaining and using another person’s personal data in some way that involves fraud or deception, typically for economic gain.</td>
</tr>
<tr>
<td>Software Piracy</td>
<td>The unauthorized copying/distribution of software.</td>
</tr>
<tr>
<td>Unauthorized Access/Hacking</td>
<td>Unauthorized, trespassing within, communicating with, stealing data from, or otherwise interfering with computer resources without explicit permission, including hacking, malware, and virus attacks.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>When an attacker floods the bandwidth or resources of a targeted system or servers with traffic, thereby preventing legitimate users from accessing information or services.</td>
</tr>
<tr>
<td>Website Defacing</td>
<td>Taking control of a web site fraudulently to either change the content of the original site or redirect the user to another false similar looking page controlled fraudulently controlled by other.</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Form of malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data “hostage” until the victim pays a ransom, frequently demanding payment in Bitcoin.</td>
</tr>
<tr>
<td>Salami Attack</td>
<td>Cyber crime usually used for the purpose of committing financial crimes in which gunners steal money or valuable assets at a time from financial accounts or systems.</td>
</tr>
<tr>
<td>Logic Bomb</td>
<td>Programming code that is hidden in a program or system that causes something to happen when the user performs a certain action or when certain conditions are met.</td>
</tr>
<tr>
<td>Data Diddling</td>
<td>Unauthorized changing of data before or during the input to a computer system. Examples are forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements.</td>
</tr>
</tbody>
</table>

Source: New Markets Lab (2018)

### B. Private-sector-led Multi-stakeholder Regulation

In addition to cybercrime legislation (top-down regulation), private-sector-led multi-stakeholder regulations (bottom-up regulation) were developed to guide private actors looking to establish preventive systems within enterprises in anticipation of possible cybersecurity risks. Under this approach, existing industry best practices (programs, guidelines, and standards) are harmonized and adopted through a multi-stakeholder framework – consisting of government, industry, academia, and international partners. For enterprises, aligning with these practices could help prioritize investment in cybersecurity, and many of these guidelines allow flexible adoption in a manner tailored to the size and nature of the enterprise.

It is important for companies to keep abreast of these practices. Even though these frameworks are voluntary in nature, non-compliance with widely adopted best practices could put them at a competitive disadvantage. As a case in point, in the US, the Cybersecurity Framework (CSF) created by the National Institute for Standards and Technology (NIST) has become a guideline and standard to establish due diligence in cybersecurity investigations. The NIST Framework is a multi-stakeholder guideline that resulted from meetings with hundreds of representatives from business, civil society, and government. The framework harmonizes industry best practices and adopts a risk-based approach to help organizations detect, mitigate, respond to cyber threats.

---


Similarly, the UK has incorporated voluntary adoption of security guidelines in its 2011 UK Cyber Security Strategy. An interesting feature of this strategy is the Cyber Essentials certification program that creates incentivizes for the adoption of basic security controls; this program is mandatory for UK government contractors handling personal information. The UK government, through Advice Sheets on the 10 Steps to Cybersecurity Program, facilitate the process by which companies (large or small) might obtain Cyber Essentials certification. Such accessibility measures are particularly beneficial to SMEs, which can use the certification as a way of enhancing consumer confidence in its products and services but are often intimidated by the technical nature of cybersecurity.

C. Comprehensive Cybersecurity Legislation

To complement cybercrime and private-sector-led multi-stakeholder frameworks, many countries have been rolling out new, more comprehensive, cybersecurity legislation. The wave of new legislation is a nod toward the growing sophistication of cybersecurity threats and carries new compliance costs. Under these frameworks, enterprises are frequently required to have certain systems, technology, or plans in place to protect security online. Those that are involved in critical infrastructures, such as electricity grids, may be subject to additional requirements for national security purposes.

Comprehensive legislation both seeks to minimize the likelihood and impact of cybersecurity incidents through preventative measures (for example, risk assessment and monitoring) and addresses issues through reactive measures (for example, responses to security breaches). Legislative approaches vary, however, in their scope and specificity. Some measures specify the underlying technology to be used (for example in South Korea, all financial transactions must be authorized using a specific encryption technology), while others do not. Greater specificity could lead to additional compliance costs (especially when an enterprise must switch from a different yet equally effective technology) and would require regulators to periodically update their regulations to reflect technological advancement. On the other hand, requiring enterprises to adopt specific technologies could help raise the industry minimum standard, as all entities have to abide by the minimum standard.

To prevent or mitigate a cyber incident or cyber attack, some regulations require government entities or enterprises to have various strategic, organizational, and monitoring mechanisms in place. In Mauritius, the Computer Emergency Response Team of Mauritius (CERT-MU), through the Botnet Tracking and Detection project, is able to take proactive measures to contain threats on different networks across the country. Additionally, the State of New York’s Department of Financial Services (DFS) directive requires companies to adopt a highly prescriptive cybersecurity program (for example, through identification of cyber risks (internal or

---

external) before they happen and creation of a defensive infrastructure to protect covered information).  

Some regulations mandate the creation of several positions within an enterprise or a government agency or the contracting of cybersecurity services to ensure cybersecurity, all of which can be costly. For example, New York’s DFS directive requires companies to have a Chief Information Security Officer (CISO). In the same vein, the draft Singapore Cybersecurity Bill calls for the appointment of a Commissioner of Cybersecurity who is responsible for the administration of the Cybersecurity Act. These obligations could make enforcement and compliance challenging, particularly for SMEs that do not always have the funds to adopt these changes within the established deadlines.

Monitoring is a central component of these efforts as well. Some jurisdictions have adopted a risk-based approach, requiring public and private entities to conduct regular risk assessment exercises and monitoring processes, periodically evaluate the effectiveness of identified controls, and adjust their control mechanisms based on their evaluation. For instance, owners of critical information in Singapore must conduct audits every three years to evaluate their compliance with the Cybersecurity Bill, carry out a cybersecurity risk assessment, and establish mechanisms and processes to detect any cybersecurity threat.

Many regulations also mandate post-cyber incident reporting and sometimes mitigation procedures. As the first step, enterprises should understand what triggers the reporting obligations or additional procedures. Some regulations use a results-oriented approach, where an event is considered a cyber incident when the information system is actually breached (this is the case in Russia, for example). Another method focuses on the attempt to breach, which is enough to constitute a cyber incident (this is true at the U.S. federal level and in some U.S. states as well as in Singapore). In terms of reporting and other mitigation procedures, regulatory provisions range from those that are silent in these respects to those that mandate prompt and detailed notifications. For instance, the U.S. federal government does not mandate incident reporting, whereas Russia requires banks to inform the Central Bank of any cyber-incident that threatens data security in payment transactions. The EU is even more prescriptive and granular in its approach. In the

---

159 The directive furthermore establishes additional requirements applicable to covered companies that set out a detailed response program.
160 New York State Department of Financial Services 23 NYCRR 500, Section 500.4.
161 Singapore Cybersecurity Bill Article 16.
163 The Federal government defines incident as “an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system” 6 USC § 148(a)(3); the New York State Department of Financial Services regulation defines a cybersecurity event as “any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.”
164 The Singapore Cybersecurity Bill defines “cybersecurity incident” as an act or activity on or through a computer or computer system, that jeopardized or adversely impacted, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, 10 confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system.
165 Cybersecurity Act of 2015.
EU, legislation has evolved to mandate incident reporting for some sectors, such as in the telecom industry and for digital service providers. The EU’s Network and Information Security Directive mandates Member States to legislate cybersecurity in a manner that requires digital service providers to notify the competent national authority without undue delay of any incident having a substantial impact on the provision of a service.\footnote{Article 16 (4), NIS Directive.} While the laws themselves do not specify the reporting processes, they often identify the respective national authority that must be notified, and businesses must make sure to report to the relevant authorities in the jurisdictions in which it is mandatory.

**Implementation and Enforcement of Cybersecurity**

Having robust and resilient cybersecurity systems are critical yet challenging for public and private actors. Regulators may find it difficult to keep up with changes in relevant technology and its application. SMEs, often the primary victims of cyber-attacks, face an array of challenges to meet mandatory regulations and voluntary industry standards. A study by the Ponemon Institute in 2017 found that cyber attacks affecting SMEs had increased from 55 to 61 percent in a span of a year.\footnote{Ponemon Institute. 2017 State of Cybersecurity in Small and Medium-sized Businesses (SMB). Web. September 2017.} A majority of these attacks were phishing/social engineering and web-based. Despite the prevalence of cyber-attacks, several key issues emerged that interfere with the adoption of cybersecurity measures by SMEs. The first issue is under-investment in cybersecurity. For instance, most Singaporean SMEs spend well below one percent of their revenue on cybersecurity, the figure deemed by the World Economic Forum to be the industry average necessary for information and communications technology (ICT) industries to combat issues in the cyber-sphere. \footnote{Karl Flinders, UK SMEs have false sense of cyber security. Web. September 13, 2016.} This underinvestment is perhaps caused by SMEs’ misconception that cyber threats only affect large organizations. For example, a report by Juniper research showed that seventy-four percent of SMEs in the UK think they are safe from cyber-attacks, even though they admit to having suffered from data breaches.\footnote{Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.}

Insufficient budget is another leading cause of underinvestment by SMEs.\footnote{Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.} It can be costly for SMEs to invest in the hardware, software, and organizational transformation needed to implement relevant regulations and standards. The baseline amount required for minimum protection can easily exceed an SME’s budget, which is often pegged to revenue or ICT spending.\footnote{Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.} This baseline amount includes a perimeter defense, such as using network firewalls and installing enterprise-grade anti-malware protection in all computers being used as part of the company.\footnote{Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.} ICT personnel are also required to manage security vulnerabilities and keep systems updated with the latest software.\footnote{Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.}
Further, SMEs typically lack both security professionals and information regarding cybersecurity standards and adoption. The absence of in-house personnel often results not only in difficulty adequately protecting computer systems but also an inability to appropriately interpret technical standards and update software in a timely manner.\textsuperscript{174} This practical difficulty is exacerbated by the fact that many of the technical standards lack implementation guidelines, thereby making it difficult for SMEs to independently comply with them.\textsuperscript{175} At a systemic level, one of the reasons for such inaccessibility is the fact that standards have been developed for larger organizations, which tend to have larger budgets and dedicated cybersecurity teams. Further, SMEs are often ignored in the process of developing standards; therefore, there is a sense that technical standards do not adequately address SMEs’ issues and challenges, nor are they geared towards practices common among SMEs.\textsuperscript{176}

Relatedly, companies, especially SMEs, often do not have the expertise or awareness to select the appropriate standard required for their particular enterprises. Table 6 below lists some popular frameworks which can provide a baseline for enterprises as they choose appropriate standards. When deciding on the appropriate standards framework, enterprises should weigh the following factors: i) whether the framework applies to the business’s industry ii) the standards required for adequate protection, iii) the role of the enterprise (buyer or supplier), and iv) the context of use.\textsuperscript{177}

Table 6: Cybersecurity Standards

<table>
<thead>
<tr>
<th>Framework</th>
<th>Standard-setting Body</th>
<th>Key Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27001</td>
<td>International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)</td>
<td>• Specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system in an organization  \n• Requirements are generic and intended to be applied by all organizations regardless of type, size, or nature, which makes them widely used and recommended</td>
</tr>
<tr>
<td>Cloud Controls Matrix</td>
<td>Cloud Security Alliance</td>
<td>• Gives detailed understanding of security concepts and principles in 13 domains</td>
</tr>
<tr>
<td>NIST CSF</td>
<td>National Institute of Standards and Technology</td>
<td>• Spans functions: Identify, Protect, Detect, Respond, and Recover \n• Divides implementation into tiers, under which a company can choose how rigorous it wants its cybersecurity framework to be\textsuperscript{178}</td>
</tr>
</tbody>
</table>

Critical Security Controls  
SANS Institute

- Includes a list of 20 controls that are designed to prevent and recover from cyber-attacks – examples include: the creation of inventory and control of hardware and software assets, continuous vulnerability management, and incident response and management.\(^{179}\)

Source: New Markets Lab (2018)

**Institutional Framework Related to Cybersecurity**

Given the multi-layered and highly technical nature of cybersecurity, governments need to consider a holistic institutional framework to support the legal framework. Different functions to consider include i) legal and regulatory bodies to promulgate and implement rules and regulations, ii) technical capacity to identify, defend, respond, and manage cyber threats (examples include the National Computer Security and Incident Response Team in Rwanda and the Computer Emergency Response Team (CERT) in the EU), iii) capacity-building to raise awareness, provide training, and develop resources, and iv) cooperation among inter-agency, national-subnational, and international partners.\(^{180}\) It is not uncommon that these different functions will be housed within a single regulatory body.

In practice, some countries have in fact created a central regulatory watchdog for cybersecurity (for example, Tunisia established the National Agency for Computer Security). As depicted in Diagram 9, in the EU, the European Union Agency for Network and Information Security (ENISA) works across all functional pillars.\(^{181}\) Pending reforms of ENISA will strengthen its power in all pillars and permanently solidify ENISA’s role.

**Diagram 9. European Union’s Institutional Framework for Cybersecurity**

---

\(^{179}\) Center for Internet Security. *CIS Controls*. Web.

\(^{180}\) International Telecommunication Union. “Global Cybersecurity Index 2017.” 2017. 4.

Source: New Markets Lab (2018)

A more centralized approach streamlines oversight of different sectors, provides a single point of contact for enterprises, minimizes the potential of fragmenting rules across sectors, and avoids regulatory uncertainty and overlap, which can be common in a multi-agency approach. Given the high level of technicality inherent in cybersecurity, a centralized and specialized agency is particularly critical for capacity building and coordination.

In contrast, the US has a more decentralized institutional arrangement, with multiple agencies with authority over cybersecurity. Compliance under this approach can be challenging for enterprises, due to duplication, conflicts, and confusion among rules and guidelines, especially since sub-national regulators often put in place more detailed and stringent requirements. For instance, financial institutions in the state of New York must comply with both the DFS Directive and Federal Gramm-Leach-Bliley Act (GLBA) that require financial institutions to implement safeguard measures to ensure secure storage and transmission of customer data.182 The federal and state approaches establish similar obligations (for example, the adoption of a written security program) but have different minimum standards.183 These layers of regulation mean that institutions must make a difficult determination with regard to compliance or potentially spend more resources attempting to comply with both standards.

**International Framework for Cybersecurity**

Globally, countries tend to regulate cybersecurity differently, and there is not a binding set of international rules that would harmonize national systems. International frameworks, which include conventions, initiatives, and trade agreements, tend to center around international cooperation and capacity building and are generally non-prescriptive. Table 7 sketches out the key international frameworks relating to cybersecurity.

<table>
<thead>
<tr>
<th>Framework</th>
<th>Key Provisions and/or Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multilateral</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Budapest Convention United Nations Groups of Governmental Experts on Information Security184 | • Harmonizes domestic criminal laws concerning cybercrime, while also providing guidelines for enacting domestic criminal procedures  
• Addresses offenses against confidentiality, integrity, and availability of computer data and systems; computer-related offenses; content-related offenses; and criminal copyright infringement  
• Boosts international cooperation and global policy-making in combatting cybercrime |

184 Convention Ch II sec. 1 title 1-4
### WTO General Agreement on Trade and Services (GATS Agreement)
- Requires non-discriminatory treatment and transparency once a country has made commitments to open domestic sectors to international trade

### Regional

| Organization for Security and Co-operation in Europe (OSCE) | Creates confidence-building measures, which offer mechanisms that bring together states to de-escalate rising tensions, platforms for information-sharing, and ways to tackle security threats from organized criminals and terrorists |
| Shanghai Cooperation Organization – International Code of Conduct for Information Security | Addresses cyber-conflict, such as cybercrime and terrorist use of ICT, as well as internet governance issues, surveillance, and content policy in the Draft International Code of Conduct for Information Security |
| Organization of American States (OAS) – Comprehensive Inter-American Cybersecurity Strategy | Develops a regional warning network to alert and inform about incidents across OAS states |
| | Shares secure infrastructure for managing CSIRT communications with the private sector and other stakeholders |
| | Supports OAS Member States with the drafting of their cybersecurity laws and capacity building exercises |
| ASEAN Regional Forum - Work Plan on Security of and in the Use of Information and Communications Technologies | Enhances cooperation across the region, including regular drills across the states |
| | Tests and enhance incident response and broader cooperation among ASEAN CERT through the ASEAN Computer Emergency Response Team Incident Drill |
| United Nations Office on Drugs and Crime/ITU Memorandum | Offers technical assistance and legal training |
| CPTPP | Recognizes the importance of cooperation on cybersecurity matters |

**Source:** New Markets Lab (2018)

### Key Takeaways for Cybersecurity

While e-commerce has been able to deliver inclusive growth, vulnerabilities on the Internet and constantly evolving technologies require a robust and resilient cybersecurity system. Regulations

---

189 Note that since, the Guidelines have been replaced by the Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. *See OECD, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* Web. 1 October 2015.
190 International Telecommunication Union.
in this field have evolved, and public and private actors could work in concert to determine the appropriate regulatory balance and sequencing of reform, taking into consideration the compliance burden of enterprises, particularly SMEs, and needs of consumers.

Cybercrime legislation, which criminalizes a range of cybercrimes, can be effective when accompanied by appropriate sanctions and strong enforcement capabilities. Alignment with industry best practices that are harmonized and sometimes adopted through public-private initiatives could help enterprises focus and prioritize investment decisions (particularly for SMEs with limited capacity and underinvest in cybersecurity). Importantly, enterprises could participate in the standard-making and harmonization process to ensure that their needs are addressed (for example, recognition of equivalence of existing standards). In any case, overly prescriptive standards may present challenges for SMEs, which would best benefit from a system that allows for flexibility in adopting relevant standards. Regulators could also create incentives for enterprises to adopt best practices (for example, SMEs can benefit from certifications that enhance consumer confidence). Finally, the recent movement towards enactment of comprehensive regulations with preventive and reactive aspects should be considered in terms of the hardware, software, and organizational requirements that will be placed on SMEs.

Institutional arrangements also have important implications for compliance. A single regulator, which is the global trend, could help provide a unified point of contact for enterprises, streamline rules and regulations, and avoid duplication of function or other issues that may arise from overlapping regulations. At the sub-national level, regulators will likely continue to roll out more stringent and detailed rules and standards, which will strengthen cybersecurity and also create additional compliance obligations.
Chapter IV Consumer Protection

Consumer protection laws seek to protect the interests of consumers and foster a trustworthy e-commerce environment that could encourage more consumers to engage in online transactions. The rise of novel business models, multifaceted advertising methods, and pervasive cross-border transactions calls for public and private interventions to guarantee an equal level of protection for e-commerce as afforded to conventional trade. Enterprises that market and sell their products online are expected to comply with legal requirements at various stages of the transaction, ranging from advertisement to cancellation of orders.

One particular area that enterprises and consumers should focus on is dispute resolution, given that merchant-customer disputes frequently arise in the post-sale, or after-sale, phase. Further, SMEs in developing countries often cite compliance with consumer protection laws as a challenge for growing their digital presence.\textsuperscript{191} Despite the importance of clear consumer protection regimes for both businesses and consumers, there is little consensus on standards at the international level, and this issue should be elevated to the level of others in this Legal Guide. Consumer protection is also often one of the last areas that developing countries focus on regulating as they create frameworks around e-commerce.

\textit{Regulatory Approaches to Consumer Protection}

Regulatory distinctions across jurisdictions are generally based on two aspects of consumer protection: the allocation of responsibilities among different stakeholders (governments, industry, and consumers) and the balance between conventional consumer protection regimes and e-commerce specific regimes.

There is considerable variation in how regulatory systems assign responsibilities among industry, government, and consumers, both with respect to rule-making and enforcement. On one end of the spectrum, in Chile and the US, the courts will sometimes be used for enforcement, including through class action lawsuits.\textsuperscript{192} Some European countries have focused on policies to empower consumers with information so that they can make informed choices that drive the marketplace.\textsuperscript{193} Alternatively, China relies heavily on public actors in both rulemaking and enforcement.

Other countries are increasingly relying upon public-private partnerships. For instance, in Spain, an independent non-governmental group called Confianza Online sets standards based on EU and Spanish laws and regulations.\textsuperscript{194} Member businesses can choose to voluntarily sign on and abide by the Ethical Code (targeting advertising, e-commerce transactions, and consumer redress mechanisms), which binds them to a certain standard of care that is frequently updated to reflect


\textsuperscript{194} Confianza Online. Web
the changing legal framework.\textsuperscript{195} The key enforcement mechanisms of this system are essentially a certification – an independent review process to receive a “Trust Mark”\textsuperscript{196} – and an alternative dispute resolution system, which involves EU authorities.\textsuperscript{197}

Another rising trend is for e-commerce businesses to operate as platforms that host consumer-consumer exchanges, and countries have begun establishing regulatory and legal frameworks specifically targeted at these host businesses. Even within regimes that place a responsibility on consumers to exercise their legal rights, e-commerce platform owners should be aware of their responsibilities and liabilities, which could broadly include information verification, monitoring, and supervisory duties. This approach is often feasible for established actors but could disadvantage new entrants and SMEs. For instance, Malaysia requires third-party platforms to maintain certain business records of vendors operating on their platforms.\textsuperscript{198} Similarly, China places extensive responsibilities on e-commerce platforms (both third-party platforms that host digital stores and company-owned-and-run platforms) and even holds platforms vicariously liable when they fail to provide information on offending vendors.\textsuperscript{199} In contrast, the US and the EU have both expressly limited e-commerce platforms’ liability through legislation, thus placing more of a responsibility on the users.\textsuperscript{200}

The second issue is the balance between conventional consumer protection regimes and e-commerce specific regimes. Overall, many existing consumer protection provisions continue to apply, as they address consumer needs that are present in both online and offline transactions. Accommodating issues specific to e-commerce (for example, data protection) and taking into account existing statutory structures, some countries have either updated their existing consumer protection laws or enacted new e-commerce specific laws (for example, South Korea’s Act on Consumer Protection in Electronic Commerce).\textsuperscript{201}

More concretely, several common regulatory elements often exist in consumer protection regimes. These common elements address consumer needs at different stages of a transaction, as set out in Diagram 10. The nuances of these regulatory elements are explained in further detail below. Two of the elements, transparent/authenticated online payments, and data protection, are addressed in Chapters I and II, respectively.

\textsuperscript{195} Confianza Online, Ethical Code, Web
\textsuperscript{196} Confianza Online, Ethical Code, Web
\textsuperscript{199} Draft E-Commerce Law in China, Chapter II, Section 2, November 2017. Law of the People’s Republic of China on Protection of Consumer Rights and Interests, Article 44.
\textsuperscript{201} Korean Legislation Research Institute, Act on the Consumer Protection in Electronic Commerce, Etc. Web.
**Diagram 10. Regulatory Elements of Consumer Protection**

![Diagram showing regulatory elements of consumer protection](image)

- **Pre-purchase (Pre-contractual Phase)**
  - Duties to Disclose
  - Advertising

- **Payment (Contractual Phase)**
  - Terms & Conditions of Transactions
  - Transparent/Secure payment
  - Data Protection

- **Delivery/After-sale (Post-contractual Phase)**
  - Dispute Resolution and Redress
  - The Right to Withdraw/Cancel (Cooling-Off Period)

*Source: New Markets Lab (2018)*

**Duties to Disclose:** Many jurisdictions have designated a list of information that must be disclosed by e-commerce platforms or online vendors to ensure that consumers can make informed purchases. Covered information generally is classified as either 1) business information, such as the trader’s name and the address at which the trader is established (for example, as required within the EU); 2) mandatory product labelling, particularly for high risk products such as food; and 3) disclosure of governmental inspection results (for instance, in Wales and Northern Ireland, online food operators must display the food hygiene ratings given by public inspectors).

**Advertising:** Advertising is a common business practice present in digital and conventional commerce. Advertisements are representations made by sellers to inform and allure consumers to the sellers’ products and services, and the role of consumer protection laws is to ensure that those presentations are not misleading. In many jurisdictions, existing advertising laws continue to apply in e-commerce and are enforced via the same regulatory authorities. In the US, for example, the Federal Trade Commission (FTC) evaluates the legality of online advertisements through criteria present in conventional trade, just as it does for offline advertisements.

Two e-commerce specific advertising tactics have invited targeted regulations. The first concerns celebrity (or more broadly “influencer”) endorsement of products and services through social media. The U.S. FTC requires influencers to “clearly and conspicuously disclose their relationships to brands when promoting or endorsing products through social media.” Another newly emerged tactic is user-generated content (UGC), including consumer evaluations and ratings on websites such as Yelp (for food businesses) and TripAdvisor (for travel businesses).

---


205 Id. at 21.

To prevent e-commerce platforms from manipulating evaluations and ratings in favor of certain vendors, China’s draft E-commerce Law prohibits traders from making up UGC or deleting UGC unless they are abusive or slanderous or are obviously contrary to facts.  

**Terms & Conditions of Transactions:** The most relevant aspects of terms and conditions of digital sales for consumer protection are 1) disclosure and transparency and 2) fair terms and conditions. Disclosure and transparency requirements obligate traders to display terms and conditions that are “likely to affect a consumer’s decision regarding a transaction.” The disclosure must also be accessible and clear. For instance, in Argentina, traders need to provide clear, comprehensive, and unequivocal access to the general terms. In practice, terms and conditions can be difficult to comprehend, which hinders the intent of protection. An analysis from the UK found that 43 percent of the adult English population cannot understand Google’s 2013 terms and conditions. However, few regulations (if any) mandate the use of clear and generally comprehensible language. Therefore, enterprises could follow the OECD’s recommendation that online disclosure and its terms be made in “plain and easy-to-understand language.”

As to fair terms and conditions, “fairness” is interpreted differently across jurisdictions. While courts in the US routinely uphold standard contracts between corporations and consumers, the EU deems that a term which has not been individually negotiated (such as those that appear frequently in standard contracts) is unfair if “it causes a significant imbalance in the parties’ rights and obligations.” Consumers can and should also rely on mandatory terms and conditions that are present in some jurisdictions to seek redress. To enforce these mandatory terms and conditions, EU courts will vacate contract terms that attempt to waive or restrict them.

**Dispute Resolution and Redress:** Disputes between merchants and consumers routinely arise in e-commerce, as consumer expectation and product description are commonly not aligned. Various options and trade-offs exist in the choice of dispute resolution mechanism. Traditional court systems are not always reliable and can be a difficult forum for consumers to enforce their rights; other challenges arise due to cost; access to affordable, quality legal services; jurisdictional limits; and sometimes prolonged litigation.

In order to be informed of the range of options, consumers should first check to see if their jurisdictions have introduced special judicial processes for handling claims under a specified monetary threshold (special or small claims courts). For e-commerce transactions, Online

---

207 Draft E-Commerce Law in China, Chapter II, Section 18, 33.
209 Latin p.12.
Dispute Resolution (ODR), offered by public and private entities, can be another, faster, alternative to the conventional and slow court system. Box 4 provides some examples of ODR.

Box 4: Online Dispute Resolution

ODR has been widely promoted by governments and businesses. In Brazil, the National Consumer Secretariat, established in 2014, is an online conciliation mechanism for consumer disputes. Eighty percent of disputes on this platform are resolved within seven days. The Office of the Federal Prosecutor in Mexico runs a similar system.

In the private sector, eBay has a “Money Back Guarantee” policy that allows consumers to file an online compliant within 30 days. Once a complaint is filed, traders must respond in the “Resolution Center” or provide appropriate remedies; otherwise consumers could request eBay to step in. Other e-commerce platforms, such as Alibaba and PayPal, also have versions of ODR. Under Alibaba’s system, both sides of a dispute may submit a compliant. If the dispute is not resolved within 10 days, it will be referred to Alibaba’s ODR team for a resolution. The potential penalty for noncompliance with Alibaba’s resolution could be severe, such as the termination of accounts. Running an ODR will required highly trained professionals and may strain the capacity of SMEs.

Arbitration and mediation are also alternatives. Consumers deciding between litigation and other forms of dispute resolution (or alternative dispute resolution (ADR)) to enforce their rights should consider several factors, as should enterprises considering the use of a mandatory arbitration clause in their terms of service. These include reliability and efficiency of the local court system, availability of qualified and affordable arbitrators, confidentiality of judgments (usually preserved in arbitration), and the ability to appeal a decision (results of arbitration panel can only be appealed under limited circumstances). In the case of cross-jurisdictional contract disputes, arbitration is viewed as more neutral towards foreign parties and may be the preferred option to litigation in domestic courts, although arbitration can be expensive for consumers and small enterprises. Binding mediation is another form of ADR, which may have application in the e-commerce context.

Right to Withdraw/Cancel (Cooling-off period): Because inspecting products prior to purchase is more difficult in e-commerce, consumers are more vulnerable to deceptive marketing. Thus, some regulators have stepped in to provide consumers with the right to cancel their orders, otherwise referred to as the right to withdraw or a cooling-off period (this period is 7 working days in the EU, 7 days in China, 5 days in Singapore, and 10 days in Malaysia). Some regulators have additionally imposed a minimum price, below which the right to withdraw cannot be exercised ($25 at the federal level in the US, for example). Enterprises should also

---

218 Consumers’ Rights and Interests Protection Law of the People’s Republic of China (PRC), Section 25.
check to see if their products fall under one of the exceptions to the right to withdraw (for example, exceptions could include personalized goods, perishable goods, or digital content).\(^\text{220}\)

**Implementation and Enforcement of Consumer Protection**

While transactions can be international, enforcement is local. Divergent consumer protection laws, jurisdictional limitations, language barriers, and inadequate cooperation between law enforcement across jurisdictions can create a number of challenges.

Language differences complicate implementation and enforcement challenges in the cross-border context. Requirements for Duties to Disclose might be well understood in a local or regional market but will not necessarily translate in the global market. The literal translation of online platforms is also an issue, especially for industries without common standards and terminology. Not every company has the capacity to translate a webpage into the language of consumers or fully anticipate consumers’ needs. For law enforcement and juridical processes, obtaining and having parties agree to translations of a given document (for example, terms and conditions of transactions) can be costly and time-consuming.

The degree to which law enforcement officials in different jurisdiction cooperate is another determinant of effective enforcement. Some nations have begun working together to improve consumers’ ability to fight illegal activity. For example, the U.S. SAFE WEB Act addresses this problem by authorizing the FTC to provide additional information to foreign governments that makes it easier for those governments to prosecute consumer protection claims.\(^\text{221}\) Likewise, the FTC can accept and use more information provided by foreign governments. There are also online platforms such as econsumer.gov, where consumers can specifically file cross-border complaints. Forms are offered in multiple languages, making it easier for consumers to use them.

**Institutional Framework Related to Consumer Protection**

In many jurisdictions, a central regulator with broad legislative and oversight mandates is tasked with consumer protection.\(^\text{222}\) This centralized approach can minimize overlapping regulatory mandates, ensure consistent policies, and reduce potential conflicts between rules promulgated by different agencies.\(^\text{223}\) Examples of this approach include the Denmark Consumer Ombudsman institution, the Ministry of Industry, Investment, Trade and Digital Economy in Morocco, and the National Consumer Commission in South Africa. Notably, due to the close linkages between competition policy and consumer protection,\(^\text{224}\) some primary consumer protection regulators are also competition regulators (for example, the Competition and Markets Authority in the UK and the FTC in the US).\(^\text{225}\) Some jurisdictions have adopted a sectoral approach, which could allow

\[^{220}\text{European Commission, Regulation (EC) 1169/2011, Article 16.}\]
\[^{221}\text{FTC, the US SAFE WEB Act: The First Three Years. December 2009.}\]
\[^{223}\text{Consumer Affairs Victoria, Institutional arrangements for consumer protection agencies. Web. April 2008.}\]
\[^{224}\text{Id.}\]
\[^{225}\text{See CMA (UK), About Us. Web; FTC, about the FTC, web.}\]
regulators to develop deeper expertise in their regulated industry and respond to industry-specific regulatory needs (for example, Australia and Norway).\textsuperscript{226}

Notably, while the institutional frameworks governing consumer protection in the online and offline spheres are generally identical, some countries have founded special enforcement units to strengthen enforcement in the digital world, particularly in high-risk areas such as food. This approach recognizes that the Internet poses special enforcement challenges and thus requires an updated enforcement apparatus, including hardware and software, expert staff who can exercise public surveillance without being identified public authorities, and enforcement officials who are apt at collecting digital evidence. Germany is a case point, as elaborated in Box 5.

**Box 5. The G@ZIELT™ in Germany**

In Germany, the G@ZIELT™ was established as a permanent unit in 2013 for "control of food, feed, cosmetics, consumer goods and tobacco products traded on the Internet" by the Federal Office of Consumer Protection and Food Safety and the 16 German Federal States. Unlike the traditional German food control system that heavily depends on states, G@ZIELT™, as a federal unit, searches for unregistered food businesses and high-risk food sold online and then passes surveillance results to states. The European Commission considers the German system a best practice, and it is a reference for good practices more broadly.

Sources: European Commission and Slovak Presidency of the Council of the EU, *Food Chain in the Digital Single Market (Introduction to the Programme of the conference)*; Panteia/CSES, *Good practice in market surveillance activities related to non-food consumer products sold online*.

**International Framework for Consumer Protection**

International initiatives generally do not prescribe specific measures for consumer protection, and further attention in this area could achieve two important goals. First, international guidelines could be helpful for identifying core consumer rights and concerns and therefore areas where regulation may be needed. Second, an international framework could help encourage cooperation among governments, improve enforcement, and enable knowledge sharing of different ways to address challenges. Table 8 lays out current international initiatives.

**Table 8. International Framework for Consumer Protection**

<table>
<thead>
<tr>
<th>Initiatives</th>
<th>Main Provisions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Multilateral</strong></td>
<td></td>
</tr>
<tr>
<td>OECD Guidelines for Consumer Protection in E-commerce\textsuperscript{227}</td>
<td>• Covers consumer-to-consumer transactions&lt;br&gt;• Expands on enforceability and investigation actions\textsuperscript{228}</td>
</tr>
<tr>
<td>The United Nations Guideline for</td>
<td>• Requires UN Member States to continue developing transparent and effective policies that ensure equal protection across all forms of commerce\textsuperscript{229}</td>
</tr>
</tbody>
</table>


\textsuperscript{228} EU’s new CCP regulation to strengthen enforcement power could be an indicator. See European Commission: *Regulation (EC) No. 2017/2394*, December 2017.
### Consumer Protection

- Calls for existing policies to accommodate special features of electronic commerce
- Calls for the recognition of rights and obligations in digital marketplaces
- Encourages multinational cooperation on cross-border e-commerce and refer to the OECD Recommendation

| UNCITRAL Model Law on E-Commerce | Mentions consumer protection, but does not expand on specific obligations |
| The International Consumer Protection and Enforcement Network (ICPEN) | Facilitates information exchange, Publishes guidelines, Provides online scams complaint site |

### Regional

- Consumer Protection Cooperation (CPC) Framework (2007) (Updated version was adopted on 2017 and will enter into force 2020)
  - Promotes effective enforcement in cross-border cases
  - Enables consumer protection agency in one CPC Member State from the EU and European Economic Area to require counterpart from other Member States to intervene and take measures to stop protection breach
  - Allows authorities to shut down suspicious sites or social media accounts (in the updated version)
  - Adopts a more centralized mechanism, where the CPC Commission will have powers to directly initiate non-compliance actions

| European Consumer Centers Network (ECC-Net) | Serves as an advisory center for consumer protection rights and obligations |
| ASEAN Strategic Action Plan for Consumer Protection (ASAPCP) | Establishes a common consumer protection framework, Ensures a high level of consumer empowerment and protection, Improves consumer trust, Integrates ASEAN consumer protection policies, Establishes an ASEAN Regional ODR Network |
| Digital Agenda for Latin America and the Caribbean (eLAC2018) | Aims to adapt consumer protection regulations to the digital environment |

**Source:** New Markets Lab (2018)

---

231 Id. Section 64.
232 Id. Section 65.
235 ICPEN in partnership with consumer agencies from 35 countries runs the complaint site.
242 Id.
Key Takeaways for Consumer Protection

Consumer protection in e-commerce is essential to fostering a trustworthy e-commerce environment and engaging consumers in online transactions. Having a strong consumer protection regime in place can benefit enterprises and consumers alike. An important question for any consumer protection regime is how responsibilities are allocated across regulators, industry (particularly e-commerce platforms and online vendors), and consumers. Depending on the specific conditions in a country (for example, market conditions and the court system), different regulatory approaches may be suitable.

The question of liability for e-commerce platforms is increasingly being raised. Heavy obligations, such as information verification and supervision, might be efficient in markets with high market concentration but could disadvantage new entrants and SMEs in smaller, more fragmented markets.

Consumer protection regimes tend to follow the different stages of a transaction. Understanding relevant regulations applicable to each stage and engaging in self-regulation in accordance with enterprises’ capacities could add to brand quality, further increase the likelihood consumer engagement, and minimize reputational fallouts in case of a dispute. Enterprises should also examine whether there are e-commerce-specific business aspects that may not be covered by the existing regulatory regime (for example, advertising through social media).

One area in which enterprises and consumers share an interest is in dispute resolution, as merchant-customer disputes routinely arise in the post-sale phase. Enterprises often designate a dispute mechanism in their terms of service. Ultimately, the choice among litigation, arbitration, mediation, and ODR will depend upon several factors such as capacity, the reliability of local courts, and international or domestic nature of the dispute (for example, arbitration or mediation may be more feasible for cross-border disputes due to language and judicial neutrality concerns). Enterprises should evaluate access to small claims court system or ODR that are speedy, affordable, and particularly suited to address online merchant-customer disputes.

Internationally, consumer protection in e-commerce has not received the focus it deserves. While a number of initiatives exist, they tend to be general in nature and do not provide sufficient guidance to enterprises, governments, or consumers. Going forward, this may be an area in which a model law could be helpful, as could greater integration with the other areas of law and regulation covered in this Legal Guide.