SEPTEMBER 2021

mourant

UPDATE

BVI electronic transactions legislation

A new set of British Virgin Islands (**BVI**) legislation has come into force to modernise and enhance the legal framework relating to electronic signatures, electronic transactions and electronic commerce.

Background

The Electronic Transactions Act, 2021, the Electronic Transfer of Funds Act, 2021 and the Electronic Filing Act, 2021 came into force on 9 July 2021. These new acts modernise and enhance the acceptance and use of electronic signatures (**e-signatures**) and electronic transactions (**e-transactions**) in the BVI and recognise and facilitate technological developments in electronic commerce (**e-commerce**).

A summary of some key elements of each act is set out below.

Electronic Transactions Act, 2021 (ETA)

The ETA, which repeals and replaces the Electronic Transactions Act, 2001, provides the framework for the facilitation and regulation of electronic communications (**e-communications**) and e-transactions

The ETA does not require any person to use or accept e-communications, e-signatures or electronic contracts. It also does not prohibit parties engaged in a transaction that are using electronic means from agreeing to vary any provisions under Parts II (requirements for legal recognition), III (electronic contacts) and IV (secure electronic signatures and records) of the ETA. The parties can establish reasonable requirements relating to the manner in which e-communications, e-signatures or electronic forms of documents may be accepted. However, the ETA codifies that a transaction conducted using electronic means will not be denied legal effect or validity solely due to the type or method of e-communication, e-signature or electronic authentication chosen by the parties to that transaction.

Exclusions

The ETA does *not* apply to a limited number of documents with special execution formalities under BVI law (eg wills, contracts for the transfer of interest in real or personal property, powers of attorney and deeds). These documents will still require traditional 'wet ink' signatures.

Legal recognition of electronic information communications

As a general rule, information[1] will not be denied legal effect or validity solely because it is in the form of an e-communication or is not in an e-communication purporting to give rise to such legal effect but is referred to in that e-communication.

[1] **Information** includes data, texts, documents, records, electronic records, images, sounds, codes, computer programmes, software and databases (s.2(1), the ETA).

The ETA sets out the requirements for the legal recognition of information provided electronically where a BVI law requires:

- information to be in writing or in printed form;
- the provision of information in a prescribed paper or other non-electronic form;
- the provision of access to information in paper or other non-electronic form;
- the delivery, dispatch or service of information on a person;
- the presentation or retention of information in its original form; and/or
- the retention of documents, records or information.

Affixing seals and notarising documents

Where a seal is required by law to be affixed to a document and that law does not prescribe how that document may be sealed electronically, the ETA provides that the sealing requirement will be satisfied if the document indicates that it is required to be under seal and includes the 'secure electronic signature' (see below) of the person who is required to seal it.

Where a law or agreement requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, this requirement will be satisfied if the e-signature of the notary, verifier or other relevant person is attached to the e-signature or electronic record, along with all information required to be included by any other applicable law.

Admissibility of electronic communications

An electronic record or e-signature will not be denied admissibility in evidence in court, tribunal or arbitration proceedings solely because it is in the form of an e-communication.

Legal recognition of electronic contracts

A contract will not be denied legal effect or validity solely on the ground that an e-communication is used in its formation. Unless otherwise agreed by the parties, an offer, or the acceptance of the offer, or any matter that is material to the formation or operation of a contract, may be expressed by means of e-communications.

In addition, a declaration of intent or other statement between the sender and the addressee of an e-communication will not be denied legal effect or validity solely because it is in the form of an e-communication.

Time and place of dispatch and receipt of electronic communications

An e-communication will be:

- treated as sent when it leaves an information system under the sender's control (or, if it has not left an information system under the sender's control, when the e-communication is received);
- treated as received when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee (or, if it has not been sent to such a designated address, when the addressee becomes aware that the e-communication has been sent to that address and it becomes capable of being retrieved by the addressee at that address);
- deemed to be sent at the place where the sender has its place of business; and
- deemed to be received at the place where the addressee has its place of business.

Contracts formed using automated message systems[2]

Where a contract is formed by the interaction between an automated message system and a person, or by the interaction of automated message systems, it will not be denied legal effect or validity solely because a person did not review or intervene in each of the actions carried out by the automated message system or the resulting contract.

---

[2] **Automated message system** means a computer programme or an electronic or other automated means used to initiate an action, or respond to electronic communication or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the programme or other automated means (s.2(1), the ETA).

If a person makes an input error in an e-communication exchanged with another party's automated message system and the automated message system does not allow the person to correct the error, that person has the right to withdraw the portion of the e-communication in which the input error was made provided that they:

(a) notify the other party of the error as soon as possible; and

(b) have not used or received any material benefit or value from any goods or services received from the other party.

Secure electronic signatures and records

Electronic signatures

Where a law or agreement requires a signature, the signature requirement will be satisfied in relation to an e-communication if:

(a) a method is used to identify the person and to indicate that the person intended to sign or otherwise adopt the information in the e-communication; and

(b) the method used is:

  (i) as reliable as appropriate for the purpose for which the e-communication was generated or communicated in the light of all the circumstances (including any relevant agreement); or

  (ii) proven to have fulfilled the functions described in paragraph (a) above, by itself or together with further evidence.

If the parties to an e-transaction require an e-signature and they have not agreed on the type of e-signature to be used, the ETA also sets outs a list of conditions for satisfying the signature requirement. However, a party is still able to establish the reliability of an e-signature in another way or adduce evidence of the non-reliability of an e-signature.

Unless otherwise provided by law, parties to an e-transaction may agree to use any particular method or form of e-signature or security procedure.

Recognition of foreign certificates and e-signatures

An authenticating certificate,[3] which is used to support an e-signature or authentication data (eg a user name, password and license key), will be legally effective regardless of the jurisdiction in which it is issued. Parties to transactions may agree to use any particular security procedure provider or class of security procedure provider or any class of certificates in connection with e-communications or signatures submitted to them.

Secure electronic record and secure electronic signature

Electronic records and e-signatures and will be treated as a **secure electronic record** and a **secure electronic signature** respectively, if a security procedure or a commercially reasonable security procedure agreed between the parties involved has been properly applied to verify:

(a) in the case of an electronic record, that such electronic record has not been altered since a specific point in time (in which case it will be treated as a secure electronic record from that specific point in time to the time of verification);

(b) in the case of an e-signature, that such e-signature was, at the time it was made:

  (i) unique to the person using it;

  (ii) capable of identifying such person;

  (iii) created in a manner or using a means under the sole control of the person using it; and

  (iv) linked to the electronic record to which it relates in a manner such that if the record was changed the e-signature would be invalidated,

  in which case it will be treated as a secure electronic signature.

[3] **Certificate** means an electronic record or other record which confirms the link between a signatory and the signature creation data (s.2(1), the ETA).

Whether a security procedure is commercially reasonable will be determined taking into account the purposes of the procedure and the commercial circumstances at the time of use. Relevant factors for this purpose would include the nature of the transaction, the sophistication of the parties and the number of similar transactions entered into by the parties.

Presumptions relating to secure electronic records and secure electronic signatures

In any proceedings involving a secure electronic record or secure electronic signature, the ETA presumes (unless evidence is adduced to the contrary) that:

- the secure electronic record has not been altered since the specific point in time to which the secure status relates; and
- the secure electronic signature is the signature of the person to whom it correlates and was affixed by that person with the intention of signing or approving the electronic record.

Intermediaries[4] and electronic commerce service providers[5]

Protection from liabilities

As a general rule, an intermediary or e-commerce service provider will not be subject to civil or criminal liability in respect of any information contained in an electronic record in respect of which it provides services if it was not the sender of the record and:

(a) has no actual knowledge that the information gives rise to civil or criminal liability;

(b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability of the information ought reasonably to have been known; or

(c) it follows the procedures prescribed under the ETA for dealing with unlawful or defamatory information.

No duty to monitor e-communications processed

An intermediary or e-commerce service provider has no duty to monitor any e-communication processed by means of its systems to ascertain whether its processing would constitute or give rise to civil liability.

The ETA sets out the procedures that an intermediary or e-commerce service provider should take regarding unlawful or defamatory information in an electronic record if it

- has actual knowledge that such information gives rise to civil or criminal liability; or
- is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of such information ought reasonably to have been known.

Codes of conduct and standards

Intermediaries and e-commerce service providers must comply with any applicable codes of conduct or standards specified by the relevant BVI Minister from time to time. The ETA sets out the consequences and penalties for non-compliance with any approved code of conduct or specified standard, including the giving of a cease and desist direction. Failure to comply with such a direction is an offence with liability on summary conviction to a fine of up to US$50,000 and, on the offence continuing, a further fine of US$1,000 for each day that the offence continues.

Consumer protection

Persons using e-communications to sell goods or services to consumers must provide certain prescribed information to consumers. Any person who sends unsolicited commercial e-communications to consumers in the BVI, either directly or knowingly through an intermediary, must give consumers a clearly specified and easy to activate method to opt out of receiving future communications.

---

[4] **Intermediary** with respect to an electronic communication means a person including a host who on behalf of another person, sends, receives, or stores either temporarily or permanently that electronic communication or provides related services with respect to that electronic communication, and includes telecommunication service providers, network service providers, internet service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafes (s.2(1), the ETA).

[5] **Electronic commerce service provider** means a person who uses electronic means in providing goods or services, or both (s.2(1), the ETA).

Any person who provides a consumer or a user of an e-signature with false or misleading information commits an offence and is liable: (a) on summary conviction to a fine of up to US$200,000 or up to three years' imprisonment (or both); or (b) on conviction on indictment to a fine of up to US$200,000 or up to five years' imprisonment (or both).

Electronic Transfer of Funds Act, 2021 (ETFA)

The ETFA regulates the transfer of money through electronic means such as by the use of bank or credit cards or online banking transfers and for related matters, including the authorisation of payments to/from a cardholder's account.

The ETFA creates a number of offences relating to the use of a credit card, debit card, bank card, smart card, electronic wallet or device or the number or data associated with any such card, electronic wallet or device (together, a card), including:

- theft, forgery and other dishonest, fraudulent or authorised use of such card;
- use of a false, fictitious, counterfeit, revoked or expired card; and
- fraudulent electronic fund transfers.

Subject to certain conditions, the ETFA also restricts the liability to a bank or card issuer for misuse of a card where a cardholder (or the issuer or any person authorised by a cardholder to use the card) has lost possession of their card to a sum of not more than $100.

Electronic Filing Act, 2021 (EFA)

The EFA provides for the use of electronic records and documents on transactions with public authorities. It gives flexibility for public authorities to design electronic forms for online transactions, facilitating the process between public authorities and third parties.

Among other matters, a BVI public authority that accepts filings or issues permits, licences or approvals may do so electronically.

Next steps

For more information, please contact your usual Mourant contact or get in touch with one of the named contacts below.

Contacts

Paul Christopher
Managing Partner, Mourant Ozannes
Hong Kong
+852 3995 5700
paul.christopher@mourant.com

Ian Montgomery
Partner, Mourant Ozannes
British Virgin Islands
+1 284 852 1730
ian.montgomery@mourant.com

Simon Lawrenson
Partner, Mourant Ozannes
Hong Kong
+852 3995 5707
simon.lawrenson@mourant.com

2021934/81626618/1