quickly, without being trammelled by detailed regulations or the necessity of having a lawyer at their side every step of the way. In the English context, after the Financial Services Act and the 'Guinness' and 'Blue Arrow' scandals (among others) of the last decade, one might view this attitude with some amusement; alternatively, one might hark back to the 1970s, when this attitude was prevalent, with nostalgia for a golden age. But there is no doubt that such an attitude was widespread and was encouraged by many of the US bankers, lawyers and others then operating in Europe. It was natural enough for the US lawyer in private practice to look upon the SEC (or, in the case of banks, the Comptroller of the Currency) as the organisation primarily responsible for making his and his clients' lives so difficult; and to contrast this with the apparent freedom in Europe. In addition, he must have been worn down by the chore of endlessly explaining to his European counterparts the detailed ramifications of the activities of powerful regulatory organisations of which they had no experience and knew no equivalents. As to the US bankers and securities dealers, the experience of coming to Europe in the 1970s was a culture shock which many found liberating. I can remember many questions from US bankers in the early 1970s as to whether there was any fundamental legal impediment to the transaction being proposed; to which often the reply would be—why should there be? What do you have in mind? In consequence, there were few articulate defendants of the US approach to whom Europeans were exposed; rather, they were encouraged in their faith in their own systems by the majority of US practitioners in Europe. Scandals such as the IOS affair were conveniently forgotten.

One wonders also how far this divergence in attitude was reinforced by more deep-rooted historical and cultural attitudes. Certainly, it is a commonplace assertion that to declare an act a criminal offence is to reinforce the underlying belief that it constitutes a moral wrong. Everyone knows the historical reasons why Switzerland takes so seriously the banker's duty of confidence and treats breach of it as a criminal offence. In the paper on Swiss law delivered in 1979, these reasons were stated proudly and unequivocally. It may be a sign of the times that, in the equivalent paper in this publication, the statement is more muted. There can be no doubt that in 1979 the stringency of Swiss law on this subject was highly respected and the reasons for it well understood. In a sense, Switzerland was regarded as the acme of banking rectitude.

No doubt, there was (as there still is) a strong competitive element also. There always has been and always will be a huge quantity of international money, owing allegiance to no particular country, looking for a home where secrecy is guaranteed. Switzerland's assumed success in attracting a large proportion of this money has long been regarded with envy by bankers in other countries.

There may also have been an element of assertion of cultural superiority by the old world over the new, a recurring tendency in many parts of Europe after (if not also before) the Second World War.

Many of these factors were contributing to the apparent isolation, during the 1970s, of US attitudes to banking regulation and banking secrecy from the European attitude. Certainly, this isolation was apparent from the papers delivered and views expressed at the conference in 1979. Yet, even then, the discerning observer might have perceived the beginnings of a convergence in those attitudes. The most concrete indication was, perhaps, the Treaty of 25 May 1973 between Switzerland and the US concerning mutual assistance in criminal matters, which was mentioned in almost apologetic terms by the Swiss speaker at the 1979 conference as a minor tear in the enveloping fabric of Swiss banking secrecy, yet to some appeared to drive a coach

and horses through the principle. In the United Kingdom, the Banking Act 1979 was strengthening the powers of the banking supervisors; legislation against insider trading was also mooted. This first came into effect in the Companies Act 1980.

Ten years later, one can see that a distinct shift in European attitudes has taken place. There appear to be several reasons for this. First, and perhaps foremost, the increasing globalisation of the banking and securities businesses presents a whole new range of problems to the domestic supervisors. It has become clear to them that the traditional concept of jurisdiction limited by territorial boundaries is wholly inadequate in the context of the developing global market. Simultaneously, there has been an increasing recognition of and determination to tackle the money laundering which is an inherent feature of international and organised crime. Finally, there has been a growing appreciation and acceptance, in the securities industry, of the principle of the 'integrity' of the market; in other words, that confidence in financial markets can only be preserved by the provision of simultaneous and, where possible, instantaneous access for all to all relevant information. The principal source of all these ideas has been the US. It is no longer isolated.

In the United Kingdom, the legal effect has been dramatic. As already mentioned, insider trading became a criminal offence in 1980. The attack on organised crime (particularly drug- or terrorist-related) has been stepped up to such an extent that, in one case today, a bank which merely suspects that it is handling the proceeds of crime itself commits a criminal offence if it fails to report its suspicion[2]. The investigatory powers of the authorities have been strengthened or, in the case of inquiries instituted by the Department of Trade under the Companies Acts, utilised to an extent never seen before. Market practices which, in the past, might have been considered dubious but would certainly have gone unpunished, if not undetected, have been ruthlessly stamped on. Finally, 'Big Bang'—presented as the 'deregulation' of the securities industry—has been accompanied by the Financial Services Act, under which the securities industry is now regulated to an extent it has never known before.

Although the United Kingdom would, no doubt, claim that it has worked out (and is still working out) its own solutions, the similarities between the approach of the United Kingdom and that of the US are far more striking than the differences. No doubt many reasons can be offered for this convergence of attitudes, but I will limit myself to suggesting two. The first is obvious: the much-trumpeted 'victory' of the philosophy of the free market. There is no need to enter the debate over whether or not the philosophy is right, or whether it has been victorious over competing ideologies. It is sufficient to acknowledge that in the United Kingdom, in the last decade, this philosophy has been dominant and that the one field of activity to which its principles have been applied most vigorously has been the financial sector. This is not to say that the financial sector has been opened to unrestricted free enterprise. Rather, as already noted, it has been subjected to greater regulation than ever before. There have been substantial borrowings from the longer US experience of running an economy dedicated to the free enterprise principle. The paradox is that maintenance of the free market appears to require the strictest regulation of the market participants.

The second reason is more complex, but also represents a borrowing, albeit less conscious, from US experience. The increasing internationalisation of the banking and securities industries is rapidly eroding the cultural homogeneity of local financial markets. In the United Kingdom this process is already almost complete.

2 Drug Trafficking Offences Act 1986.

where there are reasonable grounds for believing that there is in specified premises a thing connected with 'a special ACC operation/investigation' (referred to as 'things of the relevant kind') and that there could be a risk of concealment or destruction of that thing.[88] The issued warrant authorises entry for the purposes of search and seizure.

Section 28 of the ACC Act gives a member of the ACC the power to summon witnesses and to take evidence. Section 29 gives a member of the ACC the power, by notice in writing served on a person, to require that person to produce a specified document or thing specified in a notice which is relevant to an investigation that the ACC is conducting in performance of its special functions. Importantly, s 29A provides that a summons or notice issued under ss 28 or 29 may provide that disclosure of information about the summons or notice, or any connected official matter, is prohibited, except in the circumstances, if any, specified in the notation. Section 29B provides that any person served with, or otherwise given, a summons or notice containing such a notation must not disclose the existence of the summons or notice or any information about it. If a disclosure is made, the maximum penalty is 20 penalty units (currently $3,400) or imprisonment for one year.[89] For a corporation, the fine is a maximum of five times that amount, currently $17,000.

Effects on banker's duty of confidentiality

[2.26] There is no special treatment afforded to confidential information in the possession of a bank.[90] A bank in receipt of an ACC warrant or notice properly issued and served will be required to comply with it regardless of the common law duty of confidentiality. Further, s 29A would clearly prevent a bank advising an affected customer of the issue of a s 28 summons or a s 29 notice.

Commonwealth bankruptcy legislation

Requirements of the law

[2.27] The Bankruptcy Act 1966 (Cth) provides a number of methods for a trustee in bankruptcy to obtain documents. Where information is sought in relation to a bankrupt's account, the trustee in effect is acting as the bankrupt. One example is if a bank is the subject of a written direction of the 'official receiver' under the Bankruptcy Act. The 'official receiver' will be entitled at all reasonable times to full and free access to all premises and books which are the subject of the written direction.[91] Considerations that are relevant when faced with court orders to disclose information are also relevant in this context.[92]

Section 77A of the Bankruptcy Act provides a trustee, who is conducting an investigation under s 19AA in relation to a person, the power to require a person to produce, at a specified time and place, specified books or classes of books.

88 Australian Crime Commission Act 2002 (Cth), s 22.
89 Section 29B(2) provides certain circumstances in which a person is entitled to make a disclosure, including, in para (b), disclosure to a legal practitioner for the purposes of obtaining legal advice or representation relating to the summons.
90 There is an exception for documents subject to legal professional privilege in s 30(3) of the Act.
91 See the Bankruptcy Act 1966, s 77AA in regard to the official receiver's powers.
92 See the discussion under 'Disclosure Under Compulsion of Law' above.

Another example is s 125 of the Bankruptcy Act, which is specifically directed at the situation where a prescribed organisation[93] (which includes a bank) has ascertained that an account holder is an undischarged bankrupt. In that case, unless the prescribed organisation is satisfied that the account is on behalf of some other person, it must inform the trustee in bankruptcy, in writing, of the existence of the account. Further, payments out of the account are prohibited, except under an order of the court. If, within one month from the date on which the prescribed organisation informed the trustee of the existence of the account, a copy of the court order has not been served on the prescribed organisation and it has not received written instructions from the trustee, the prescribed organisation is entitled to act without regard to any claim or right the trustee may have in respect of the account.

Effects on banker's duty of confidentiality

[2.28] There is no specific exemption for banks from the operation and effect of these provisions and, therefore, they are another example of the compulsion of law exception.

Other statutory provisions

[2.29] Other State and Commonwealth legislation may also limit the protection provided by the principles in *Tournier*. In many cases, this arises out of reporting obligations to regulatory authorities or the power of regulatory authorities to enter and search premises and to compel the production of documents. Some key examples of such legislation have already been covered separately above, but other examples of such Commonwealth legislation include the Banking Act 1959 and the Life Insurance Act 1995. Other examples of such state legislation include the Estate Agents Act 1980 (Vic), Legal Profession Act 2004 (Vic) and the New South Wales Crime Commission Act 2012 (NSW).[94]

A bank that discloses information to a regulator pursuant to such legislation may be concerned with the potential for that regulator to further disclose that information to other agencies. In *Johns v Australian Securities Commission*,[95] the High Court considered the issue of regulators disclosing information obtained from a person or company to another regulator. On this subject, Justice Brennan commented:

> 'A statute which confers a power to obtain information for a purpose defines, expressly or impliedly, the purpose for which the information when obtained can be used or disclosed. The statute imposes on the person who obtains information in exercise of the power a duty not to disclose the information obtained except for that purpose … The person obtaining information in exercise of such a statutory power must therefore treat the information obtained as confidential whether or not the information is otherwise of a confidential nature.'

However, relevant legislation may expressly permit a regulator to make further disclosures of that information. For example the ACC Act, in particular see ss 19A and 20, gives the ACC powers to seek information from Commonwealth agencies,

93 Prescribed organisation is defined to include a bank in s 125(3).
94 Statutes from Victoria and New South Wales are chosen as an illustration of legislation which exists at a state level.
95 (1993) 178 CLR 408.

with the relevant provisions of the bi- and multilateral conventions.[52] Therefore, administrative assistance in foreign tax assessment procedures also has to be provided in cases which are subject to Austrian bank secrecy. Formerly, information was only exchanged with respect to criminal fiscal proceedings concerning intentional tax evasion (*Steuerhinterziehung*). In addition, such proceedings had to be initiated in a qualified manner prior to the release of bank information. The ADG's purpose, pursuant to its preamble, is the 'implementation of the OECD-principles regarding the bilateral exchange of information'. The determination of the extent of information that must be exchanged is up to the respective double tax treaty, EC legislation or international agreements (eg, a Tax Information Exchange Agreement – TIEA). Hence, the extent of exchange is subject to bilateral relationships.

The standard of information exchange set out in Article 26(5) of the OECD Model Tax Convention provides that any information, including bank account details, that is 'foreseeably relevant' for purposes of the administration and enforcement of tax laws (not only criminal tax laws) must be exchanged. 'Fishing expeditions' are not covered – there is no obligation to automatically and abruptly exchange information. Further, the request for information may only be sent after domestic procedures in the requesting country did not provide for sufficient information. The bank, the persons affected, as well as the relevant account must be explicitly named.

The ADG provides for a legal remedy in connection with the information exchange. The person whose bank details are obtained must be informed immediately after the Austrian authorities have determined that, generally, an information exchange procedure is legitimate. The affected person may within two weeks request a formal ruling from the authorities stating reasons why bank details might be passed on to foreign authorities. This ruling can subsequently be appealed against at the Administrative Court (*Verwaltungsgerichtshof*) or the Constitutional Court (*Verfassungsgerichtshof*). The information exchange procedure is halted until the respective court has rendered a decision. Only the persons affected can challenge the exchange of information, not the banks.

Agreement between the United States of America and the Republic of Austria for Co-operation to Facilitate the Implementation of FATCA

[3.24] On 29 April 2014 Austria and the United States of America entered into an agreement for the co-operation to facilitate the implementation of the Foreign Account Tax Compliance Act ('FATCA') based on direct reporting by Austrian financial institutions to the US Internal Revenue Service ('IRS'), supplemented by the exchange of information upon request pursuant to the Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income between Austria and the United States dated 31 May 1996.

The agreement, which corresponds to the American 'Model 2' agreement authorises and obliges Austrian financial institutions to disclose aggregate information (Sammeldaten) to the IRS of Non-Consenting US Accounts (ie accounts held by customers with a US nexus who do not consent to the disclosure of their federal taxpayer ID to the IRS).

52 *Flora*, Praxisrelevante Fragen zu Auskünften nach dem ADG (2014) ÖBA at 3.

This aggregate information may give rise to subsequent group requests to the Austrian tax authorities. Upon such group request the individual and detailed information may be forwarded to the IRS.

Summary

[3.25] Austrian authorities do not render legal assistance to foreign authorities in civil matters if such assistance is contrary to bank secrecy. Austria will render legal assistance in criminal matters in accordance with applicable treaties or the ARHG even if that requires a lifting of bank secrecy, provided the requirements for and the limits to a lifting of bank secrecy are fulfilled. If provided for in applicable treaties, such (foreign) criminal matters may include fiscal offences and both requesting authorities and authorities rendering legal assistance may be administrative agencies as well. By way of the ADG Austria grants full access to bank information in case of requests for information from foreign tax administrations if such information is 'foreseeably relevant' for purposes of the administration and enforcement of tax laws. However, due to the international pressure, Austria agreed to the extension of the Council Directive 2003/48/EC on Taxation of Savings Income and therefore intends to abolish the Austrian bank secrecy for foreigners by the year 2017 and to implement an automatic exchange of information with foreign tax authorities. Furthermore, Austria entered into an agreement with the United States of America for cooperation to facilitate the implementation of the Foreign Account Tax Compliance Act based on direct reporting by Austrian financial institutions to the IRS, supplemented by the exchange of information which as a result has significantly curtailed the Austrian bank secrecy in respect to US account holders.

Money laundering and financing of terrorism

[3.26] According to a report of the IMF in 2004, Austria has a high level of observance of internationally accepted standards in the area of anti-money laundering. Section 38(2), no 2 of the BWG provides for an exception of banks' duty to confidentiality by reference to BWG, s 41(1), (1a) and (2) which set out certain disclosure obligations if a transaction raises suspicion or if there is a legitimate reason to assume that such transaction serves for purposes of money laundering or financing of terrorism. Basically, s 41 provides as follows:

1 If there is suspicion or a legitimate reason to assume that: (i) a transaction, which has already occurred, is in progress or is about to occur, serves for the purpose of money laundering (s 165 of the Austrian Criminal Code (*Strafgesetzbuch* – 'StGB')); or (ii) any capital asset is derived from money laundering; or (iii) a client has breached its duty to disclose fiduciary relationships pursuant to BWG, s 40(2); or (iv) a transaction, which has already occurred, is in progress or is about to occur, or any capital asset relates to a criminal organisation (StGB, s 278), a terrorist organisation (StGB, s 278b), a terrorist crime (StGB, s 278c) or serves the purpose of financing terrorism (StGB, s 278d), banks (including finance institutions) shall, without delay, inform the relevant authority (to be determined according to the Austrian Security Police Act) and shall, until the case has been solved, stop any further execution of the transaction unless there is danger that a delay in the transaction would complicate or obstruct the investigation of the case.

Failure to make full and sufficient disclosure may lead to penalties in terms of adjournments, costs, and in extreme cases, the striking out or dismissal of a case,[8] or even committal for contempt of court.[9]

Witness summons and third party disclosure

[5.5] The obligation to provide disclosure generally only applies to the company which is a party to the proceedings (the 'bank party'). The court also has the power to order non-parties to litigation to provide evidence to the court, whether oral testimony or documentary evidence, if it is relevant to the issues that the court has to resolve. Once more, non-disclosure on grounds of legal professional privilege or public policy will be protected. If the proceedings are arbitration proceedings, the tribunal will have to rely on the coercive powers of the court with power over the witness.

The court should be sensitive to commercial and client confidentiality and will be prepared in an appropriate case to introduce measures to protect it. However, if the evidence is relevant to the issues and necessary for a fair determination of the dispute, an order for its disclosure is likely to be made.

Witness summonses cannot be used to obtain generalised disclosure from a third party or as a means of enquiring whether a bank has documentation that may be relevant.

Disclosure orders

[5.6] There are other circumstances where the common law provides that a bank may be required to provide disclosure of information that it holds. In *Norwich Pharmacal Co v Commissioner of Customs and Excise*,[10] the House of Lords established the principle that a third party may be under a duty to assist a person who has been wronged by giving him full information and disclosing the identity of the wrongdoers. This will apply whenever a person has become involved in wrongful conduct which infringes another's legal rights.

Compulsion by statute

[5.7] Most of the statutory provisions entitle the relevant body to compel a bank to produce information relevant to any matter which it is authorised to investigate. Other provisions require a bank to disclose information to the appropriate authority of its own volition on suspicion of the commission of certain criminal offences. The following list of statutory provisions is not exhaustive.

Once disclosure has been made to an authority, the information disclosed becomes subject to different degrees of protection in the hands of that body. This is established either by the applicable statutory provisions or case law. For example, information provided to the Bermuda Monetary Authority pursuant to their statutory powers is subject to a strict code on its disclosure, making improper disclosure a criminal

8 RSC, Ord 24, r 16(1).
9 RSC, Ord 24, r 16(3).
10 [1974] AC 133.

offence. Information provided to insolvency practitioners, on the other hand, is much more loosely protected. When a bank is required to disclose information, it is worth considering the degree of protection of the information in the hands of the recipient.

Police and other criminal investigations

[5.8] Recent years have seen a spate of new legislation in this area. Notably, anti-money laundering and anti-terrorism legislation requires banks to disclose confidential information if there are reasonable grounds to believe that a customer is engaged in any one of a number of specified offences or upon suspicion of money laundering.

Problems can then be caused for banks (and others) by their related statutory obligations not to pay out moneys pursuant to their client's instructions pending authorisation from the authorities and not to 'tip off' individuals whom they suspect of such offences. The following is a summary of some of the legislation relating to criminal investigations.

Money laundering

[5.9] The Proceeds of Crime Act 1997 (as amended) ('POCA'), the Proceeds of Crime (Anti-Money Laundering and Combating Terrorist Financing) Regulations 2008 (the 'Regulations'), the Anti-Terrorism (Financial and Other Measures) Act 2004 (as amended) (the 'ATF Act') and the Financial Intelligence Act 2007 (as amended), provide the central framework for Bermuda's anti-money laundering ('AML') and counter financing of terrorism regime providing a cohesive and comprehensive code aimed at the prevention, discouragement, detection and prosecution of money laundering and terrorist financing related offences in Bermuda.

The AML regime applies to financial institutions, including banks, acting in the course of business carried on by them in or from Bermuda. The core obligations of financial institutions are to establish and maintain adequate and appropriate policies and procedures to forestall and prevent operations relating to money laundering and terrorist financing.

To assist in the fight against financial crime, in 2008, Bermuda established the Financial Intelligence Agency (the 'FIA'). The FIA was established by the Financial Intelligence Agency Act 2007 (the 'FIA Act') to act as an independent agency authorised to receive, gather, store, analyse and disseminate information relating to suspected proceeds of crime and potential financing of terrorism received in the form of Suspicious Activity Reports ('SARs'). The FIA may also disseminate such information to the Bermuda Police Service and foreign financial intelligence authorities.

Bermuda law imposes a duty of vigilance on banks, including their employees, which requires the following:

1 verification of the identity of the client (or 'know your client' procedures);
2 monitoring, recognising and reporting of suspicious transactions;
3 keeping of certain records for the time period prescribed; and
4 training of employees and staff.

Investment fund operators and fund administrators are required to appoint a Money Laundering Reporting Officer ('Reporting Officer') to whom reports should be made

Compulsion of foreign legislation

[7.23] Disclosure of information to foreign authorities pursuant to foreign legislation may also be a valid exercise of the 'compulsion of law' exception to the bank's duty of confidentiality. In *Park v Bank of Montréal*,[99] a Korean branch of a Canadian bank disclosed, of its own volition, but pursuant to requirements of Korean legislation, information to Korean authorities regarding the illegal cross-border movement of currency from Korea. In a lawsuit in Canada, the British Columbia Supreme Court accepted the bank's argument that it had been validly compelled by a provision of Korean law to divulge the information. The disclosure made under these circumstances was thus held not to be a breach of the bank's duty of confidentiality. The converse issue, that is the effect of foreign legislation preventing disclosure on the compellability of foreign banks in domestic proceedings, is discussed later in the chapter under the 'Domestic Proceedings to Obtain Information from Foreign Banks or Branches' heading.

Public duty to disclose

[7.24] This rarely-used exception was referred to in *Tournier* in the context of preventing acts that might present a danger to the state. The decision seemed to imply that there would be a wide range of circumstances in which this exception might apply.

In a sense, the primary 'public duty' obligations come under specific legislation such as the traditional evidence legislation or the new money laundering provisions. The legislated duty in these situations relieves the bank of having to decide whether a sufficiently high public good would be served by disclosure so as to supersede the private duty to maintain confidentiality. This difficult judgment, combined with the ever-broadening legislative requirements, may explain why this has been a little-used exception.[100]

This exception underlies the ever increasing array of legislative provisions imposing reporting requirements on banks and financial institutions with regards to the prevention of money laundering, terrorism financing and fraud, among others. Where such legislative provisions can be used to prevent a bank or financial institution from being the victim of such activities, there may be overlap between the 'public duty' exception and the 'bank's own interest' exception, which is discussed in para **[7.5]** of this chapter.

99 1997 CanLII 3128 (BC SC) [*Park*].

100 In *Canadian Imperial Bank of Commerce v Sayani* (1993), 83 BCLR (2d) 167, BCCA, the Court of Appeal held that a bank's disclosure of a customer's indebtedness to the bank to prevent a trust company's reliance on the customer's misrepresentation of its indebtedness was a valid exercise of the public duty exception. In *Murano v Bank of Montreal* (1995), 31 CBR (3d), 20 BLR (2d) 61, Ont HCJ, affd (1998), 41 OR (3d) 222, 163 DLR (4th) 21, 41 BLR (2d) 10, 5 CBR (4th) 57, 111 OAC 242, Ont CA, disclosure by a bank to its customer's other creditors that the customer was 'dishonest' was held to fall outside of the 'public duty to disclose' exception.

In *BMP Global Distribution Inc v Bank of Nova Scotia*, [2005] BCJ No 1662, BCSC, the bank had collected a counterfeit cheque for its customers. The BC Court of Appeal allowed the appeal and the Supreme Court of Canada reaffirmed the decision of the appeal court. Because the cheque had been settled by the drawee bank, the Supreme Court held that the collecting bank was never at a loss position and thus could not invoke the 'bank's own interest' exception to divulge information about its customers in a grid warning to other financial institutions. It further held that because its customers were never under investigation for fraud, it could not claim protection of the 'public duty to disclose' exception either.

It is interesting to note that courts have upheld provisions such as those described above, even in light of challenges pursuant to s. 8 of the Canadian Charter of Rights and Freedom,[101] namely the right to be secure against unreasonable search and seizure. In *Royal Bank v Ren*,[102] the Ontario Court of Appeal upheld a decision ruling that the provisions of PIPEDA, discussed below, authorising the Royal Bank and the Toronto Dominion Bank to disclose to the Bank Crime Prevention and Investigation Office of the Canadian Bankers Association, a listed investigative body pursuant to s 26 of PIPEDA, personal information relating to a customer without the latter's consent where the banks had reasonable ground to believe that the information relates to a breach of an agreement or a contravention to the laws of Canada, a province or a foreign jurisdiction did not attract Charter scrutiny. In so doing, the court stated:

> 'In such circumstances, where reasonable grounds exist to believe that a private entity has been, is, or is about to be defrauded, limited information sharing between private business organizations and private investigative bodies is permitted for the purpose of preserving and protecting the economic interests of the business enterprise at risk. From what we can tell, the impugned provisions of PIPEDA do little more than codify the existing common law which permitted the sharing of such information in similar circumstances: see *Canadian Imperial Bank of Commerce v Sayani* (1993), 83 BCLR (2d) 167 (BC CA), at paras. 18-32.'[103]

Common law developments limiting disclosure

[7.25] As previously indicated, subsequent common law developments have further qualified the four *Tournier* exceptions, in particular, the 'compulsion of law' exception and the steps that banks are expected to take when disclosing information without its customer's consent pursuant to those exceptions. The Privy Council appears to have expanded the scope of a bank's obligation to its customer when the bank is presented with a legally enforceable demand by a third party for information about the customer. In *Robertson v Canadian Imperial Bank of Commerce*,[104] a case in which the original action was heard by the High Court of Justice of St Vincent and the Grenadines, the Privy Council held that a bank has the following additional obligations in such a situation:

1 when a bank receives a demand for information about a customer from a third party, the bank must use its best efforts to inform the customer of the demand, unless the legal authorities have requested that the bank refrain from such notification; and
2 a bank must exercise care to give only that information that is specifically required by and relevant to the inquiry.

The factual background of the case involved a previous collection action, in which a subpoena *duces tecum* was issued to the Canadian Imperial Bank of Commerce ('CIBC') with respect to the accounts of a customer in order to show that a cheque had been deposited to the customer's account. The manager of the CIBC branch attended in court with a monthly statement of the customer's account, which showed numerous other transactions, including an overdraft, that were not relevant to the action. Following the collection action, the customer sued CIBC for breach of

101 Part 1 of the Constitution Act, 1982.

102 2009 ONCA 48.

103 2009 ONCA 48 at para 22.

104 [1995] 1 All ER 824, [1994] 1 WLR 1493, PC.

7 by or to the relevant professional person with the approval of the Financial Secretary when necessary for the protection of himself of any other person against crime.

The CRPL also includes a blanket exemption where the disclosure is made in accordance with the procedures set out in the CRPL itself or any other law.

Most of the reported decisions relating to the application of the CRPL relate to the first gateway set out above, providing for the disclosure of information before a court, tribunal or other authority where such information is to be given in evidence in proceedings (known as the 'section 4 gateway'). In such cases, the professional person is obliged to make application to the Grand Court for directions on whether and to what extent to make such disclosure.

An application under the section 4 gateway is made by way of summons which must be supported by an affidavit by the applicant setting out the circumstances in which the evidence is proposed to be given, the principal of the information and the basis of the confidential relationship, the nature of the evidence, and the grounds on which the principal objects to the proposed disclosure. The application will be heard by a judge of the Grand Court sitting alone and in chambers (rather than in the public court rooms).

The judge is required to consider the interests of justice (in a criminal case) and public policy, any offer of compensation or indemnity, and whether an order would operate as a denial of the rights of any person in the enforcement of a just claim.[7]

The leading case on the section 4 gateway is *Re Ansbacher*,[8] where the court held that:

> '… [T]he Court is called upon to weigh the competing interests and decide, in the exercise of its discretion, whether and if so how [confidential information should be disclosed in evidence] having regard to the requirements of the administration of justice in the proceedings to which the application relates.'

Section 4 does not empower the court to grant a positive injunction order prohibiting the disclosure of confidential information. The court may only give directions as to whether or not, and if so on what conditions, confidential information may be given into evidence. If injunctive relief is sought, it should be claimed otherwise than under this section. Note, however, that where the proposed disclosure is in the context of the giving of evidence in proceedings the courts will prefer to deal with the matter under the section 4 gateway.

In making an order under section 4, the court will consider whether the names of the parties or other particulars ought to be redacted, whether references to names could be anonymised, whether the disclosure should occur only before certain individuals in controlled circumstances (eg before a court in person rather than by written affidavit) and whether evidence should be given in chambers rather than open court.

Note that the section 4 gateway applies only in the context of proceedings (as that term is normally understood) before a court, tribunal or other authority. This gateway is not appropriate for use where evidence is sought under an investigative power with a view to building or developing evidence for use in a hypothetical or future proceeding.

7 CRPL, s 4(6).
8 *Re Ansbacher (Cayman) Ltd* [2001] CILR 269.

There is no jurisdiction under section 4 for the court to award costs to the principal in the successful challenge to a disclosure application.

There are several reported decisions under s 4 of the CRPL that offer guidance on how the law will be applied in the context of bank confidentiality. In *Re Ansbacher*, a Cayman Islands bank applied to the court of directions under s 4 in relation to disclosure of confidential information in proceedings in Ireland. The bank had been served with an order from the Irish High Court authorising an investigation into allegations that its affairs had been conducted with the intent to defraud its clients' creditors by tax evasion. The order authorised the court's inspectors to examine the business activities of Ansbacher in Ireland. The bank wished to assist in the investigation by disclosing confidential information which would include some of its clients' identities and applied to the court for directions. Some of Ansbacher's clients objected on the basis that such disclosure would be an invasion of privacy and a breach of the duty of confidentiality owed to them by the bank.

The Attorney General, which must be served with all s 4 applications in case a matter of public interest is raised, submitted that the public interest would be secured by assisting the Irish inspectors with their investigation as they were exercising similar duties to those of the CIMA. The court accepted that there was a public interest to protect, and held that the bank should disclose the requested information subject to the condition that clients' identities be concealed. Any questions that the investigators required the individual clients to address should be issued to those clients in writing and these clients could respond anonymously.

Re Ansbacher was distinguished in the recent case *In the Matter of the Confidential Relationships (Preservation) Law (2009 Revision)*,[9] a decision of the Grand Court made in April of 2013. In that case, an English bank with its head office in London was served with a production order made by a court under the Proceeds of Crime Act of England. The production order issued to the bank stated that it was made on the application of a Detective Constable of the Metropolitan Police and required the production of a broad range of banking information. The bank made a section 4 application with respect to the material sought that arose in or was brought into the Cayman Islands. The court found that there was no 'proceeding' underlying the request for confidential information. There was indeed an investigation underway through which the police were seeking evidence to determine whether or not a proceeding should take place. However, no charges had been laid, nor any proceedings in a court, tribunal or other authority commenced. As such, the s 4 exception could not be applied. The bank's argument that the disclosure should be permitted as the failure to do so would damage the bank's reputation was also rejected. The court agreed that while disclosure is permitted in proceedings where it may be necessary to protect the bank's own interest, this gateway only applied where the bank was a party to the proceedings in question. The application was dismissed as a fishing expedition.

In *UBS (Bahamas) Ltd v Weybridge and Barclays Bank plc*[10] the court held that it would not make an order for discovery conferring on the recipient a discretion to use disclosed materials in any foreign proceedings to pursue a related claim. It was held that such an order would override the implied duty not to use discovered information for purposes other than the proceedings at hand and would conflict with the principle that the court has no automatic remit over matters outside of its jurisdiction. The court must be satisfied that such further use is warranted. When an application is

9 Unreported at the time of publication.
10 [1998] CILR N-8.

and rendering information on the request of another authority (ie the banking or administrative authority), the procedure in both situations will be very similar.

Disclosure of confidential information at a court's request

[11.24] Under principles of Czech law, legal assistance in relation to foreign countries may be provided either on the basis of generally applicable EU regulations and directives within the EU countries or in accordance with an international treaty or upon a reciprocity principle if an international treaty with the relevant country does not exist. Basically, legal relations between countries with different jurisdictions are regulated by the Act on International Private Law (no 91/2012 Coll, as amended), which, inter alia, sets out basic principles of international legal assistance. In addition to this Act, a number of treaties on legal assistance exist between the Czech Republic and other countries. In addition to the generally applicable EU regulations and directives, the Czech Republic is also a signatory to some multilateral international treaties, for instance, the European Treaty on Legal Assistance in Criminal Matters.

In principle, a foreign court may approach a bank in the Czech Republic, when seeking confidential information, only after complying with certain requirements stipulated either by the Act on International Private and Proceedings Law or by the relevant EU regulation or international treaty.

The treaties on legal assistance also usually designate the authorities of the relevant countries involved, which will be authorised to mediate between contacts in the provision of legal assistance. If a treaty does not exist or if the treaty does not designate the relevant authority, the procedure for the provision of the legal assistance and the relevant authorities involved are regulated by the Instructions of the Ministry of Justice in respect of civil law matters and commercial law matters and the Instructions of the Ministry of Justice and of the Supreme State Attorney in respect of criminal law matters, issued and updated on a regular basis. These Instructions also regulate formal steps to be taken in the process of requesting the international legal assistance. In any case, different regimes apply depending on whether or not the provision of confidential information is requested by the courts or other judicial authorities within the EU or out of the EU and also whether or not an international treaty between the Czech Republic and the relevant country exists.

Examples of procedure in connection with the disclosure of confidential information at a court's request

[11.25] In order to clarify this, some typical examples are as follows:

1 the easiest procedure applies in the event that the requesting court belongs to one of the EU member states. In such a case, the courts may, within the relevant EU regulations, contact the courts in other EU member states either directly or through the consulates of the relevant state;

2 if, however, a court in a country outside of the EU with which the Czech Republic has not entered into any treaty on legal assistance requests confidential information, the request of the court or other judicial authority must be submitted to the relevant country's Ministry of Justice (or a similar authority). The ministry will pass this request to the Ministry of Foreign Affairs (or a similar authority). The Ministry of Foreign Affairs will then forward the request to the Ministry of Foreign Affairs of the Czech Republic and this ministry will pass the request to the Ministry of Justice of the Czech Republic, which will eventually serve the request on the relevant court for a settlement, ie depending on other circumstances mentioned below, the court may request the bank to provide it with confidential information;

3 in the event that a treaty on legal assistance exists, the procedure would depend on the regulation of the mutual contacts between the relevant authorities of the two countries. Provided that the contacts are at ministerial level, the requests of the courts or other judicial authorities are delivered by the Ministry of Justice (or by an authority with a similar capacity) of the relevant country to the Ministry of Justice of the Czech Republic. The Ministry of Justice will then serve the request on the relevant court;

4 in the event that the mutual contacts between the two countries are at a consular level, the Ministry of Justice or a similar authority of the relevant foreign country will forward the request to the Ministry of Foreign Affairs (or a similar authority) and this ministry will pass the request to the consulate of the relevant country in the Czech Republic. The consulate will then serve the request directly on the court in the Czech Republic. Depending upon the other circumstances, the court may request that the bank provide confidential information.

The same procedure will apply in reverse when a court in the Czech Republic requests confidential information from a bank abroad.

Therefore, the whole procedure regarding the means of delivering the request to the relevant court in the Czech Republic depends on:

(a) whether or not the relevant court is that of an EU member state,
(b) whether a treaty on mutual legal assistance exists and also whether the treaty covers the spheres of both civil and criminal law or only one of these, and
(c) how the contacts between the two countries have been regulated, ie which state authorities have to be involved in the delivery process.

The delivery of the request, however, forms only a part of the total of all legal steps to be taken and considered in connection with the provision of confidential bank information to a foreign court.

Provided that all of the procedures for delivery of the request as described above have been duly completed, a Czech court will provide legal assistance on the request of a foreign judicial authority only on condition that: (i) the relevant EU regulation exists within the EU member states; or (ii) reciprocity exists between the Czech Republic and the relevant country. Reciprocity may be based either on a treaty on mutual legal assistance or, in the event that such a treaty does not exist or that the existing treaty does not regulate reciprocity, on mutual practice between the two countries.

The delivery and serving of requests for legal assistance or for a provision or securing of evidence in civil and commercial matters between Czech judicial authorities and similar authorities within EU countries is regulated, for instance, by Regulation (EC) no 1393/2007 and Council Regulation (EC) no 1206/2001.

Disclosure of confidential information at the request of another foreign authority

[11.26] A similar situation will then occur if another foreign authority, other than the courts, requests confidential bank information.

Compulsion by statute

[13.15] Most of the statutory provisions entitle the relevant body to compel a bank to produce information relevant to any matter which it is authorised to investigate. Other provisions require a bank to disclose information to the appropriate authority of its own volition on suspicion of the commission of certain criminal offences. Banks are also required to carry out inquiries as to the identity and suitability of a potential customer and to consider the source of funds and, in particular, whether they are derived from illegal activities. The penalties for failure to comply are set out in each statute. The following list of statutory provisions is not exhaustive.

Once disclosure has been made to an authority, the information disclosed becomes subject to different degrees of protection in the hands of that body. This is established either by the applicable statutory provisions or case law. For example, information provided to the Financial Conduct Authority ('FCA') pursuant to its statutory powers is subject to a strict code on its disclosure, making improper disclosure a criminal offence. Information provided to insolvency practitioners, on the other hand, is much more loosely protected. When a bank is required to disclose information, it is worth considering the degree of protection of the information in the hands of the recipient.

However, when considering information in the hands of a public authority such as the FCA or the Department for Business Innovation & Skills, the Freedom of Information Act 2000 must be taken into account. Under this Act, a person has the power to request and be provided with information. Information provided to a public authority protected by statute (such as the Financial Services and Markets Act 2000) or provided in confidence is exempt from the requirement to disclose. The Information Commissioner is conservative in allowing the confidence exemption. It must be clear that the information is really confidential and the ambit of the claim to confidence can be no wider. It is therefore advisable to make sure that any information provided to a public authority is specifically provided in circumstances imposing obligations of confidentiality. There are other circumstances, such as the prejudice to commercial interests, that provide a qualified exemption, in which case the authority must justify the application of the exemption on the basis that the public interest in maintaining the exemption overrides the public interest in disclosing the information. Privilege also only qualifies for a qualified exemption, but the Information Commissioner or the First-tier Tribunal (Information Rights) would be reluctant to override it. The protection afforded by legal privilege has been described by the courts as a fundamental human right.

Income Taxes Act 2007 and Finance Act 2008

[13.16] Section 748 of the Income Taxes Act 2007 ('ITA') (previously s 745 of the Income and Corporation Taxes Act 1988 ('ICTA')) gives HM Revenue & Customs ('HMRC') wide investigatory powers if it suspects non-compliance with the provisions in Chapter 2 of Part 13 of ITA regarding tax avoidance through transfer of assets abroad (previously ss 739 and 740 of ICTA). These provisions concern the avoidance of UK income tax by individuals ordinarily resident in the UK which arises through or in connection with the transfer of assets outside the UK. In *Clinch v IRC*,[53] the court considered a notice served by the Commissioners under s 481 of ICTA 1970 (the predecessor to s 745 of ICTA and s 748 of ITA) on a person (Mr

53 [1973] 2 WLR 862.

Clinch) who had acted as the London representative of a Bermudan bank. The notice required Mr Clinch to provide the Inland Revenue (as it then was) with lengthy details (including the names and addresses of customers and agents and transaction details) concerning transactions involving UK customers and Bermudan entities which Mr Clinch had acted on over several years. Mr Clinch maintained that the notice was void because it was merely a 'fishing expedition' and did not sufficiently identify the customers or transactions in which the Revenue was interested. Alternatively, it was invalid because it was unduly oppressive or burdensome. The court held that, in the circumstances, the notice was valid, although the court could intervene if such a notice went substantially beyond that required to enable the Revenue to decide whether or not in their opinion tax had been evaded. The burden of proving oppression is a heavy one. Such a notice can only be served on someone in England in relation to documents and files in England.

HMRC also has other powers under the Finance Act 2008 ('FA') to oblige third parties, including banks, to disclose documents. Previously s 20 of the Taxes Management Act 1970 ('TMA') governed this area, and notices served on a bank under s 20(3) of the TMA were considered in *R v IRC, ex p Banque Internationale à Luxembourg SA*.[54] (The court also considered further notices issued under s 767C of ICTA). The Inland Revenue (as it then was) was investigating large-scale tax avoidance schemes which had been financed by the bank. At the instigation of its customers, the bank challenged the validity of the notices on various grounds, including their impingement on the privacy and right to confidentiality of the bank and its customers in breach of Art 8 of the European Convention on Human Rights. The court held that the notices were valid. As far as Art 8 was concerned, the court held that there was ample justification for the impingement, as required by Art 8(2) of the Convention, on the basis that the notices were issued according to law, in pursuit of a legitimate aim and necessary in a democratic society for the protection of the taxation system and revenue.

More recently, applications by HMRC have been upheld by the Special Commissioners where s 20 of the TMA (now FA, Sch 36, Part 1, para 1) notices were to be served on an investment bank in respect of UK customers who were thought to be conducting share transactions via a British Virgin Islands company and on a financial institution in respect of customers with UK addresses holding non-UK bank accounts.[55] Of particular interest in these cases is the fact that HMRC was able to issue the s 20 notice without being able to name the taxpayer(s).

Since then, four Special Commissioner's rulings required four unconnected financial institutions to provide HMRC with details of UK resident customers with overseas bank accounts, or credit cards connected to overseas bank accounts. The tax exposure was significantly larger (£150 million) than the exposures in the earlier cases.

Insolvency Act 1986 and other insolvency matters

[13.17] Section 236 of the Insolvency Act 1986 applies where an administration order is made in relation to a company, an administrative receiver is appointed, a company goes into voluntary liquidation, a provisional liquidator is appointed or a winding-up order has been made by the court. The court has the power to summon

54 [2000] STC 708.

55 For decisions on share transactions, see SpC533 (2006) and SpC537 (2006) and for decisions on offshore bank accounts and credit cards, see SpC517 (2006) and SpC536 (2006).

Scientific research

[14.10] Despite the duty of non-disclosure, a bank may disclose confidential information for the purposes of scientific research, provided that the disclosed documents are at least 60 years old. In addition, the recipient of confidential information must assure in writing that the information will not be used to harm the persons or infringe the rights of persons affected by such documents.

Legal proceedings

Legal proceedings involving the bank as a party

[14.11] Despite the duty of non-disclosure, a bank may disclose to the court confidential information in connection with legal proceedings conducted by the customer against the bank or initiated by the bank against the customer (for instance, proceedings for collecting moneys owed by the customer to the bank). However, the disclosure is only allowed to the extent necessary in respect of each particular case.

If the bank litigates against its customer, the employee or official of the bank may, without the consent of such customer, disclose confidential information relating to such customer as a witness. In addition, other information subject to bank confidentiality may be disclosed if it is necessary for solving the matter.

Legal proceedings involving third parties

[14.12] In addition, a bank may be involved in legal proceedings, for example, where the customers of the bank or a third party and the customer of the bank are parties to such proceedings.

The Procedural Code provides that a witness, such as an employee of the bank, has the right to refuse to disclose information to the court in connection with civil or criminal proceedings if such disclosure may lead to prosecution against the witness himself or persons close to him, as specified in the Procedural Code. The Procedural Code further provides that a witness has a right to refuse to disclose information related to a business or trade secret unless 'fundamentally significant reasons' require such disclosure. In practice, such fundamentally significant reasons may be deemed to exist in cases where, for example, an innocent person would be convicted for a crime without disclosure of such information. Thus, it is unlikely that the witness's right to refuse to disclose a business or trade secret would be overridden in civil proceedings by application of such 'fundamentally significant reasons' test. Furthermore, the witness is entitled to disclose confidential information if the customer has consented. Before giving testimony, the witness must declare that he is under the bank confidentiality obligation.

Under the Procedural Code, if a witness refuses to make the disclosure as described above, he must give pertinent grounds for the refusal. However, this may sometimes mean that, when explaining the reasons for the refusal, the witness would then release confidential information.

If the court orders the witness to disclose confidential information, it may decide that the witness shall be heard behind closed doors. In such a case, the court may declare

that the trial documents which contain confidential information shall be kept secret for a fixed period of time.

The above also applies in cases where a confidential document is to be presented to the court or the employee or official of the bank is to be heard as an expert in court proceedings.

Arbitration proceedings

[14.13] Under the Act on Arbitration Proceedings 1992, arbitrators can hear the parties, witnesses and experts (however, without taking an oath) and receive documents that may have relevance as evidence in arbitration proceedings. Nevertheless, the arbitrators are not vested with the power to impose conditional fines or use coercive measures in order to force the persons to testify or present evidence. The court of arbitration may, however, seek assistance from the ordinary courts. Where the parties, witnesses or experts are heard or evidence is presented before the ordinary courts in connection with arbitration proceedings, the above general rules that apply to the disclosure of confidential information in ordinary court proceedings also apply to the disclosure in arbitration proceedings.

Disclosure to authorities

Tax authorities

[14.14] According to the provisions of the Act on Taxation Procedure 1995, the Finnish tax authorities enjoy extensive rights to obtain, for the purposes of assessing taxes, confidential information on payments or transfers made by a person and the adjustments made to such payments or transfers, the identity of the recipient of such payments and transfers and the grounds for such payments and transfers. Specific disclosure provisions apply to securities intermediaries as to the trades made and the derivative contracts concluded, to credit and financial institutions as to loans granted and interest paid and to asset management companies for collective investment funds as to units owned by a person and the units redeemed.

Furthermore, the obligation to disclose information applies, generally, to third parties, like banks, as regards such information which may be relevant for tax assessment or dealing with a tax appeal and which information can be identified on the basis of a name, bank account details, an identified banking transaction or other similar means of identification. This obligation is based on a specified request made by the tax authorities and covers all such information which is in the possession of or otherwise known to a person, except for such information which the person is not entitled to disclose under the provisions of the Procedural Code.

In addition, a number of provisions in various specific tax statutes and international agreements, including the Foreign Account Tax Compliance Act ('FATCA') Agreement, further specify the right of the tax authorities to obtain information. The scope of the information to be disclosed may thus depend on the particular tax statute or international agreement which is applied in the individual case. However, information may only be disclosed to the extent necessary for the tax authorities to discharge their duties in connection with the taxation under the specific tax agreement or statute.

irrelevant. Even an implicit release which can be deduced from the customer's behaviour will suffice.

If the customer did not consent expressly or where the bank has no knowledge of circumstances giving indications regarding the customer's actual wish, the bank may assume that the customer's actual wish corresponds to the hypothetical wish of a reasonable average customer. In the latter case, the bank would have to determine what objectively is in the interest of the customer.[28]

The SCHUFA-System

[16.17] The so-called 'SCHUFA' used to be a particular case in which the customer's consent was deemed to be given generally in advance. The SCHUFA is an entity set up by banks and other enterprises that regularly give credit to their customers. From its partners and public registers, the SCHUFA collects information regarding people's creditworthiness. The partners are obliged to transmit information about their customers to the SCHUFA in a standard format containing factual information about the customer relationship. The importance of SCHUFA can be gauged by the fact that debt collection agencies regularly threaten the (alleged) debtors with the transmission of their data to the SCHUFA and thereby can expect better payment behaviour of the debtors. In that regard, the Higher Regional Court (*Oberlandesgericht*) of Celle held that the threat of a data transmission to SCHUFA by a debt collection agency was not permitted if the alleged debtor had already contested the claim.[29] Nevertheless, the court has thus not objected to the widespread practice of threatening debtors with transmitting their data to the SCHUFA. The information given to and received by the SCHUFA does not contain any information about the financial circumstances of a person or an evaluation of his creditworthiness. The SCHUFA passes on information relating to a certain person if the requesting partner has demonstrated a legitimate interest in the information and the person has agreed to the collection of the information. In the past, the bank's customer was generally asked to declare his consent to that procedure in advance when, for example, a banking contract was concluded. This approach was assessed critically by the legislator since, in practice, it was nearly impossible to open a bank account or to apply for a loan without this consenting clause. As a consequence, the consent was considered not to be given voluntarily. For that reason, this procedure was restricted by the introduction of s 28a, para 2 of the Federal Data Protection Act, which provides an express statutory exception to the secrecy obligation in particular with respect to the banking sector that allows, in principle, the transfer of data to the SCHUFA (see 'Statutory exceptions' 'Data Protection' below).

Cheques, bills of exchange and debit entries

[16.18] Implied consent can usually be assumed when cheques are drawn. Before making a demand for payment, the payee usually asks the bank if it deems the cheque payable. The positive answer is that the bank considers the drawer's bank account sufficient to the payment on the cheque. The bank is entitled to reveal this information since drawing a cheque implies that the drawer reveals both the existence of a bank account and a corresponding capacity.

28 Bruchner/Krepold, n 8 above, s 39 n 10.
29 OLG Celle in GRURPrax 2014, p 93.

If the bank does not pay the cheque, it is entitled to disclose any information on the drawer necessary for the collection of the debt. That is justified on the assumption that the drawer has tacitly consented to disclosure guaranteeing smooth processing of his cheques.[30]

On the other hand, permission to perform debit entries (without the use of cheques) does not include an implied consent to answer a request on the bank account. While the cheque is drawn for a certain sum, permission to perform debit entries is generally given for several debit entries in advance and furthermore depends on the issuance of an invoice prior to the transaction.[31]

Banking information

Definition

[16.19] Banking information is an instrument that has been developed between banks to share reliable information about the creditworthiness of their business partners. Clause 2, para 2 of the General Business Conditions defines what type of information may be provided. The rule covers general statements on the banking relationship, comments as to the financial circumstances, and an evaluation of the creditworthiness of the bank's customer. Unlike in the SCHUFA system, the information must not contain specific data. The only exception to this rule is when a bank possesses information concerning cheques returned unpaid or complaints about bills.[32] Banking information will be provided not only to other banks, but also to clients of a bank.

Although a legal duty of disclosure is commonly denied, there is – at least *vis-à-vis* other banks – a corresponding trade custom to provide the required information. The bank is only obliged to transmit information currently available; a duty to conduct further investigation does not exist. It must, however, furnish true and complete information it possesses about its clients.[33] If it negligently breaches this duty, it will be liable for damages. When passing on information, the bank has to do so concisely, diffuse answers have to be avoided, and any answer has to get straight to the point, revealing no information which is not essential to the enquiry in question.[34]

Preconditions of disclosure

[16.20] Clause 2, para 3 of the General Business Conditions lays down different requirements for two types of bank clients: business persons and others. Business persons are all legal entities and natural persons which are registered in the Commercial Register and whose banking relationship can be attributed to the professional sector. Regarding these customers, banking information is considered a trade custom; business persons are assumed to know of, and to have consented to, the disclosure through implied conduct. However, a business person can object to this procedure and instruct its bank to keep the banking information secret. It will then be

30 Bruchner/Krepold, n 8 above, s 39 n 38.
31 Bruchner/Krepold, n 8 above, s 39 n 40.
32 BGH in WM 1962, p 1110 at 1111.
33 BGH in ZIP 1999, p 275.
34 Claussen, n 2 above, s 3 n 22.

further supported by a non-statutory code of conduct.[5] Accordingly, like a number of common law jurisdictions,[6] the principles established by the English Court of Appeal in the landmark case *Tournier v National Provincial and Union Bank of England*[7] remains the leading authority. The principles set out in the *Tournier* case are explained in detail in Chapter 13, England. This chapter does not intend to repeat such commentary, but rather focusses on the extent to which those principles have been adopted within a Hong Kong context.

Although the Hong Kong courts have affirmed the principles established in the *Tournier* case on a number of occasions,[8] the duty of secrecy has been significantly eroded particularly following a number of legislative enactments that have been promulgated to meet international standards. In Hong Kong, a large number of statutory provisions now exist that compel disclosure, some of which are discussed in this chapter below.

Policy considerations

[19.2] In the *Tournier* era, bank secrecy was deemed to be the cornerstone of banking and it was quite acceptable for a customer to expect a high degree of secrecy regarding information held by their banker. A high level of bank secrecy was maintained in Hong Kong until around 2012. Due to the proliferation of cross-border crime, corruption, financial abuses and terrorist activities, the international community, led largely by the developed nations in the form of the Group of 20 Nations ('G20'), Financial Action Task Force ('FATF') and the Organisation for Economic Co-operation and Development ('OECD'), bank secrecy is regarded as undesirable and has been weakened. The campaign to end bank secrecy has been particularly high on the agenda of the international community since the onset of the global financial crisis in 2008 in an attempt to replace revenue that was used to rescue national economies.

At the time of writing, bank secrecy is regarded as an extremely sensitive political and public issue on a global level, and major changes are taking place in many jurisdictions – including Hong Kong. Recent lobbying by public interest groups such as the Tax Justice Network and Oxfam[9] campaign for greater financial transparency by raising public awareness; and such campaigns have generated a great deal of public support.[10]

Despite radical changes to bank secrecy in many European countries over the past few years, Hong Kong was initially reluctant to amend its bank secrecy laws. However, particularly since 2008 the legal regime in Hong Kong has received a

5 The Code of Banking Practice, issued jointly by the Hong Kong Association of Banks (HKAB) and the Deposit Taking Company Association (DTCA), and endorsed by the Hong Kong Monetary Authority (HKMA) (effective from 2 January 2009) at http://www.hkma.gov.hk/media/eng/doc/code_eng.pdf last viewed on 14 August 2014.

6 The duty is also based in the Common law in Australia, Canada, England, Ireland, and South Africa.

7 *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461 (the *Tournier* case).

8 For example see *FDC Company Ltd v The Chase Manhattan Bank N A* [1990] 1 HKLR 277, and *Nanus Asia Co Inc v Standard Chartered Bank* [1990] HKLR 396.

9 Oxfam International, 'Tax on the 'private' billions now stashed away in havens enough to end extreme world poverty twice over' (21 May 2013). This report is at www.oxfam.org/en/eu/press room/pressrelease/2013-05-22/tax-havens-private-billions-could-end-extreme-poverty-twice-over last viewed on 10 August 2014.

10 Tax Justice Network ('TJN'), at www.taxjustice.net/cms/front_content.php?idcat=2&lang=1 last viewed on 14 April 2014.

great deal of criticism from the international community for maintaining strict bank secrecy rules that could be manipulated to assist money laundering, terrorist financing and shield international tax evasion. Hong Kong is a member of both FATF and OECD in its own right. Accordingly, FATF has made several recommendations to the Hong Kong government to bring Hong Kong legislation in line with national standards to detect and prevent money laundering and terrorist financing.[11] Although Hong Kong has never been deemed an unco-operative tax haven by the OECD,[12] the Global Forum on Transparency and Exchange of Information for Tax Purposes ('the Global Forum') has set out a number of measures that need to be implemented to ensure that Hong Kong is fully compliant with international standards, following a recent Phase 2 review.[13] Hong Kong has taken on board such recommendations and is making a concerted effort to update legislation and conclude agreements with relevant trading partners to implement the minimum standards.

The media has also become an active force in raising public awareness as to the undesirable use of bank secrecy laws to protect wealthy individuals from both legal and moral obligations. For example, a string of recent reports published in January 2014 by the International Consortium of Investigative Journalists ('ICIJ') has exposed many powerful citizens of China, Hong Kong and Taiwan as holders of offshore bank accounts and trust vehicles.[14] It is not illegal per se in Hong Kong to deposit money offshore, but the ICIJ claim that the use of offshore banking facilities and trust vehicles is often tied to 'conflict of interest and covert use of government power'.[15]

Recent initiatives to enhance tax transparency under the Foreign Account Tax Compliance Act ('FATCA')[16] regime, once fully implemented, will have a significant impact upon the duty of bank secrecy in Hong Kong and reflect the boldest move to date in the erosion of bank secrecy in Hong Kong. The government of Hong Kong has been engaged in discussions with the US Department of Treasury, with the objective of concluding an inter-governmental agreement ('IGA') designed to facilitate compliance with FATCA by Foreign Financial Institutions ('FFIs') in Hong Kong. At the time of writing Hong Kong has not yet formally concluded an IGA with

11 FATF, 'Mutual Evaluation of Hong Kong – 4th Follow-up Report' FATF Publication (19 October 2012) at http://www.fatf-gafi.org/media/fatf/documents/reports/Follow%20up%20report%20MER%20Hong%20Kong%20China.pdf last viewed 14 August 2014.

12 OECD, 'List of Uncooperative Tax Havens' the official OECD website at www.oecd.org/countries/liechtenstein/listofunco-operativetaxhavens.htm last viewed on 10 August 2014.

13 OECD, Global Forum on Transparency and Exchange of Information for Tax Purposes, Tax Transparency, 2013 Report on Progress, (2013) and OECD, Global Forum on Transparency and Exchange of Information for Tax Purposes Peer Reviews: Hong Kong, China: 2013, 'Phase 2: Implementation of the Standard in Practice' (November 2013, reflecting the legal and regulatory framework in August 2013).

14 'Leaked Records Reveal Offshore Holdings of China's Elite' *International Consortium of Investigative Journalism*, (23 January 2014) available at the official website of International Consortium of Journalism at www.icij.org/offshore/leaked-records-reveal-offshore-holdings-chinas-elite last viewed on 20 August 2014.

15 'Leaked Records Reveal Offshore Holdings of China's Elite' *International Consortium of Investigative Journalism*, (23 January 2014) available at the official website of International Consortium of Journalism online at www.icij.org/offshore/leaked-records-reveal-offshore-holdings-chinas-elite last viewed on 20 August 2014.

16 The United States, Foreign Account Tax Compliance Act (FATCA) was enacted in 2010 by Congress as part of the Hiring Incentives to Restore Employment (HIRE) Act. On 18 March 2010, the Hiring Incentives to Restore Employment Act of 2010, Public Law 111-147 (the HIRE Act), added Chapter 4 to Subtitle A, comprised of ss 1471 through 1474, to the Code. These provisions were originally introduced as part of the Foreign Account Tax Compliance Act of 2009 (HR 3933).

1 a declaration of the infringement;
2 the cessation of the infringement and ordering the other party to restrain from further infringement;
3 a remedy in the form of a public statement;
4 the cessation of the injurious status and the restoration of the previous status; and
5 transferring the financial gain acquired by the unlawful conduct in accordance with the rules of unjust enrichment.

Apart from these general and potential consequences, the injured party may claim: (a) a so-called 'injury compensation' regarding the non-pecuniary (eg psychological, emotional) injury he or she suffered; and/or (b) damages. The conditions of awarding injury compensation are the same as the conditions of awarding damages, with the exception that in the case of the former it is sufficient to evidence the unlawful action only. The court determines the amount of the compensation in one lump sum, taking into account the particular circumstances of the matter.

Criminal law

[20.6] Act C of 2012 on the Criminal Code penalises the infringement of economic secrets (including, among others, bank, securities and insurance secrets). Any person who is obliged to keep an economic secret and discloses the bank secrets to any third party (unless duly authorised) with the intent of acquiring an unjustified advantage or to cause detriment to any person, commits a misdemeanour and can be sentenced to up to two years' imprisonment.

Administrative law

[20.7] In the event of the breach of any of the provisions set out in legal regulations concerning financial and auxiliary financial services (including the breach of bank secrecy), the National Bank of Hungary can impose fines and penalties (along with other measures in serious cases).

Cross-border/extra-territorial issues

[20.8] In addition to the cross-border aspects of bank secrecy already discussed above, sanctions may be imposed on financial institutions domiciled outside of Hungary, pursuant to the provisions of the Banking Act.

If a foreign financial institution providing cross-border services in Hungary breaches the Hungarian regulations applicable to it or if insufficiencies are detected in its operations, the National Bank of Hungary is empowered to request the financial institution to rectify the problem in compliance with such regulations. In cases where the financial institution does not rectify the insufficiency or the unlawful operation, the National Bank of Hungary can notify the relevant foreign Financial Supervisory Authority of the financial institution, requesting it to take appropriate measures. The National Bank of Hungary may also act directly if it determines that the continuance of the anomalous situation presents a serious threat to the stability of the financial system or the interests of customers.

Any information which may be required in legal proceedings outside of Hungary (and which is not covered/cannot be obtained under the Banking Act directly) may be obtained under the official legal assistance regime which may be in place with

the relevant jurisdiction either on the basis of multilateral, or bilateral agreements or mutual recognition. Legal assistance procedures are implemented by courts, but the request for assistance should normally be delivered to the ministry of foreign affairs or the ministry of justice.

Regulation of financial markets

[20.9] Financial markets in Hungary are regulated by the Banking Act, which defines the financial services and the requirements of obtaining a licence to conduct such services. The Banking Act deals with the supervision of the financial institutions and sets out the rules of bank secrecy, as well as the rules of business secrecy. On the other hand, capital markets are regulated by separate pieces of law, in particular the Capital Markets Act and the Investment Services Act (the latter is the local law implementing the MiFID). The Capital Markets Act regulates (inter alia) the rules of securities secrecy, and the issuance and distribution of securities. The insider dealing and market abuse/manipulation provisions of the Capital Markets Act are in compliance with the relevant pieces of European Union law. The Investment Act regulates the investment services set out in the MiFID and contains detailed rules of securities secrecy with a list of exemptions where data relating to securities secrecy may be disclosed to third parties.

Insider trading and market manipulation

[20.10] The Capital Markets Act has implemented the European Union legislation on insider trading and market manipulation. The regulation reflects the respective European Union law and insider trading is a criminal offence under the Criminal Code.

Since the emergence of the financial crisis (starting in the second half of 2008 in Hungary) the supervisory authority imposed fines on a number of occasions on entities as in its view the conduct of such entities resulted in market manipulation.

Conflicts of interests

[20.11] Credit institutions providing investment and auxiliary investment services besides financial services must guarantee in their internal rules that the two units are separated in order not to influence the transactions between their clients, the credit institution divisions, the credit institutions and other participants. The internal rules must determine precisely the way data is conveyed between the units and bank secrets should be available exclusively for those who need them for performing their tasks. The internal rules have to be submitted to the National Bank of Hungary.

MONEY LAUNDERING

Background

[20.12] Hungary was among the first countries in Europe which adopted laws in order strictly and effectively to prohibit money laundering. Besides the former criminal code, in 2003 a new act (the 'Money Laundering Act') became effective replacing Act XXVI of 1994 on the Prevention of Money Laundering, which already

CONSENT OF THE CUSTOMER

[22.36] The duty of confidentiality of a bank in respect of its customers' affairs may be disapplied where the customer consents to the disclosure in question. A consent for this purpose may be express or implied. In the case of implied consent, it is difficult to determine the scope of the exception and whether it applies will depend on the particular circumstances of each case. One circumstance in which implied consent to disclosure has been traditionally inferred is where the customer provides a third party with the name of its bank for the purpose of the bank providing a reference in relation to the customer. However, in view of the English Court of Appeal's decision in *Turner v Royal Bank of Scotland plc*,[142] it is unclear whether the Irish courts would consider a customer has impliedly consented. The customer's implied consent will not protect the bank if it is negligent when providing information when giving a reference.

Some banks insert express provisions in their mandates and application forms permitting them to make, in relation to dealings with customers, intra-group disclosures, disclosures to regulators (including regulators outside of Ireland) and, in a few cases, disclosures to other third parties and to a credit reference bureau. Standard home loan mortgage documentation usually contains a consent by the customer to disclosure for the purpose of a securitisation by the lender. The Code of Practice issued by the Central Bank for such transactions provides:[143]

(1) A loan secured by the mortgage of residential property may not be transferred without the written consent of the borrower. When seeking consent from either an existing or a new borrower the lender must provide a statement containing sufficient information to enable the borrower to make an informed decision. This statement, which must be cleared in advance with the Central Bank, must include a clear explanation of the implications of a transfer and how the transfer might affect the borrower. The borrower must be approached on an individual basis and given reasonable time to give or to decline to give his consent.
(2) When seeking a consent and where there is to be or where there may be an arrangement under which the original lender will service the mortgage as an agent of any transferee, the lender will confirm that the transferee's policy on the handling of arrears and in the setting of mortgage interest rates will be the same as that of the original lender, and that the original lender will handle arrears as its agent.
(3) Where the lender in the ordinary course of business would no longer have control in relation to
    (a) the setting of interest rates, and/or
    (b) determining the conduct of relations with borrowers whose mortgage payments are seriously in arrears

    the lender must seek the borrower's consent to a transfer notwithstanding any previous consent which a borrower has given.
(4) When seeking the borrower's consent to the transfer of his mortgage, as described in paragraph (3) above, the lender will provide the borrower with the following information:
    (a) the name and address of the intended transferee, and of any holding company, if applicable;

142 [1999] 2 ALL ER (Comm) 664.
143 See www.centralbank.ie – Code of Practice on the Transfer of Mortgages; the Code does not apply to a transfer within the same corporate group.

    (b) the relationship, if any, between the lender and the transferee;
    (c) a description of the intended transferee and of its business, including details of how long it has been in operation, and of its experience in the management of mortgages;
    (d) an explanation of the policy and procedures which will apply for the setting of the mortgage interest rate and for making repayments if the transfer takes place;
    (e) confirmation that in the absence of a specific consent the existing arrangements will continue to apply.
(5) The terms of the transfer agreement shall require the transferee
    (a) to allow transferred mortgages to be redeemed without charging a redemption fee or approved under s 28 of the Central Bank Act 1989.
    (b) to continue any existing mortgage protection insurance arrangements;
    (c) to allow the borrower to arrange his own house insurance;
    (d) to adhere to the principles of section 26 of the Building Societies Act 1989;
    (e) to provide to the authorities the mortgage statistics previously provided by the original lender;
    (f) to comply with this code of practice in relation to any future transfer of these mortgages.

SANCTIONS FOR CUSTOMERS

[22.37] A breach of the duty of confidentiality by a bank will result in damages being awarded to the relevant customer. In *Slattery v Friends First Life Assurance Company Ltd*[144] when assessing the level of damages, the High Court did not apply the rule in *Hadley v Baxendale*[145] or consider the House of Lords decision in *Jackson v Royal Bank of* Scotland[146] McGovern J stated:

> '121. In this case, the plaintiff has not established any special damage arising out of the breach of confidence. But that is not a bar to the plaintiff recovering damages. It is clear from such authorities as *Conway v Irish National Teachers Organisation, McIntire v Lewis [1991] 1 IR 121* and *FW v British Broadcasting Corporation (Unreported, High Court, 25th March, 1999)*, that the Court is vested with a discretion to award compensatory damages, including aggravated damages, notwithstanding any failure to explicitly plead the latter category. Indeed, it would run contrary to what McCarthy J in *McIntire v Lewis* referred to as the "dynamism that characterizes the common law" for this Court to hold itself as being artificially restricted in granting the plaintiff a remedy.
>
> 122. Aggravated damages are usefully defined by the Law Reform Commission in its consultation paper on Aggravated, Exemplary and Restitutional Damages, published in April, 1998, and cited with approval by Barr J in *FW v British Broadcasting Corporation*, as follows:
>
> "Aggravated damages are classified as a species of compensatory damages, which are awarded as additional compensation where there has been intangible injury to the interests or personality of the plaintiff, and where this injury has been caused or exacerbated by the exceptional conduct of the defendant."

144 [2013] IEHC 136.
145 (1854) 9 Excl 341.
146 [2005] 1 WLR 377.

deceased person's bank account (ie, whether disclosure of the transaction records in relation to the deceased person's bank account to a co-heir upon request without the other co-heirs' consent constitutes a breach of the duty of confidentiality).

The Supreme Court of Japan[19] held that: (i) a financial institution owes a duty to disclose the transaction records in relation to a bank account upon the request of a depositor and that such duty arises under a deposit contract; (ii) a co-heir may independently exercise the right to request a bank to disclose the transaction records in relation to a deceased person's bank account pursuant to the co-heir's status under the deposit contract succeeded to from the deceased person which is vested in all co-heirs; and (iii) as long as disclosure is limited to the co-heirs, disclosure of the transaction records in relation to the deceased person's bank account upon request by one of the co-heirs does not constitute a breach of the duty of confidentiality vis-à-vis the other co-heirs because each co-heir has the requisite status under deposit contract.

Disclosure by a syndicated loan agent

[24.16] In a syndicated loan transaction there is generally an information gap between a loan agent and the other lenders. An agent would have greater access to information about the borrower through past transactions, while the other lenders may not have any relationship other than through the syndicated loan. The other lenders have to obtain a borrower's information necessary for its credit decision through the agent. If the syndicated loan agreement has no clause under which a borrower agrees to disclose information about the borrower to the lenders, whether an agent may disclose information about the borrower to the other lenders without the borrower's consent may be an issue.

It is necessary for an agent to consider the following factors mentioned in para **[24.6]** above in determining whether to disclose the relevant confidential information about the borrower. With regard to these considerations, the following should be noted:

1 in relation to item (i), the purpose of disclosure seems justifiable because an agent generally has a right to investigate a borrower and report its findings to the lenders;
2 in relation to item (ii), information on a borrower's creditworthiness should be carefully handled;
3 in relation to item (iii), disclosing information on a borrower's creditworthiness would significantly impact the borrower;
4 in relation to item (iv), the parties to whom the information will be disclosed are banks or other financial institutions; and
5 in relation to item (v), banks or other financial institutions owe strict obligations, and, with respect to information management, are subject to a duty of confidentiality under the syndicated loan agreement.

Another issue is whether an agent owes the duty to disclose information on the borrower to lenders when it obtains information on the borrower that would affect the lenders' credit decisions. The Supreme Court of Japan[20] held that an agent has a duty to disclose information to lenders in syndicated loans under the particular case summarised as follows: (i) prior to the origination of a syndicated loan in question, a borrower's principal bank, which is also an agent of another syndicated loan (the

19 The Supreme Court of Japan (*Minshu* Vol 63, No 1, p 228) (22 January 2009).
20 The Supreme Court of Japan (*Minshu* No 242, p 1) (27 November 2012).

'Agent for Another SL'), has doubts about the correctness of the financial statements of the borrower and instructs the borrower to review the latest financial statements; (ii) the fact stated in (i) above was provided to lenders of another syndicated loan by the Agent for Another SL; and (iii) the fact stated in (ii) above was provided to the agent of the syndicated loan in question (the 'Agent for This SL') by the borrower to leave the decision as to whether the Agent for This SL should continue the origination of the syndication of loans in question with the Agent for This SL. This judgment does not affirm that an agent owes general obligations to disclose information about the borrower to lenders, and is applicable to only the particular circumstances described above. However, the argument discussed in the judgment is still useful for an analysis of whether an agent owes a duty to disclose information regarding the borrower.

Disclosure in M&A transaction

[24.17] This section looks at the question of whether a bank as a party in an M&A transaction may disclose its customer information to the counterparty of the M&A transaction.

It is necessary for a bank to consider the following factors mentioned in para **[24.6]** above in determining whether to disclose the relevant confidential information about the counterparty of an M&A transaction. With regard to these considerations, the following should be noted:

1 in relation to item (i), because M&A transactions permissible under the Companies Act (Act No 86 of 2005; as amended) inherently require the transfer of customer information to the counterparty of the M&A transaction, the purpose of disclosure is likely to be legitimate;
2 in relation to item (ii), in light of the nature of M&A transactions, disclosures of comprehensive information, including the creditworthiness of customers, should be reasonably permissible;
3 in relation to item (iii), the impact on all businesses involved should be considered;
4 in relation to item (iv), if the recipient of information is a regulated organisation such as a financial institution, disclosure is likely to be legitimate; and
5 in relation to item (v), entry into a confidentiality agreement with the recipient of information tends to make disclosure legitimate.

On the other hand, when a bank discloses information obtained as a financial advisor in an M&A transaction, it generally enters into a confidentiality agreement. In such cases, a bank should determine whether it is permitted to disclose information in accordance with the confidentiality agreement. Thus, it is prudent to stipulate at the outset the identity of the permitted recipients of confidential information in order to avoid breaching the confidentiality agreement.

SANCTIONS

[24.18] If a bank discloses information regarding a customer in violation of the duty of confidentiality and the customer suffers losses or damage due to such violation, the customer may claim for compensation in a civil lawsuit against the bank.

With details in respect of administrative sanctions by the FSA pursuant to violations under the Banking Act, please refer to para **[24.23]** below.

as well as arms trafficking, prostitution, corruption and kidnapping of minors and following implementation into Luxembourg law of the Third Money Laundering Directive[70] also cover among others, fraud, counterfeiting, environmental offences, kidnapping, theft, forgery, insider dealing and market abuse etc.[71] The rules require banks to make thorough checks and controls in order to identify the origin of funds, the identity of their clients (including the beneficial owner) and suspect transactions and prohibit (through abstention) the banker from entering into certain transactions. In order to allow and compel banks to denounce acts which might constitute money laundering, a legal exemption from bank secrecy was required and therefore introduced into the Banking Law and is today provided for in the law of 12 November 2004 relating to the fight against money laundering and financing of terrorism (the '2004 Money Laundering Law')[72] which implements EC Directive 2001/97 (Second Money Laundering Directive) as well as EC Directive 2005/60 (Third Money Laundering Directive). Since 2004, the bankers' obligations in relation to money laundering are no longer set out in the Banking Law, but are grouped in a separate law specifically dealing with money laundering aspects and which applies not only to banks and professionals of the financial sector, but also to other professions such as auditors, lawyers, notaries, estate agents and generally businesses selling high-value goods where a payment in cash is made for more than €15,000.

Pursuant to the current obligations, these professionals (including bankers), their managers and employees must fully co-operate with the authorities in charge of the fight against money laundering and financing of terrorism. In this respect, each of them must:

1 of their own initiative, inform the public prosecutor when they have knowledge, suspect or have reasons to suspect money laundering or financing of terrorism, inter alia, by reason of the person concerned, the origin of the funds, the nature, the purpose or the proceedings of the transaction; and
2 furnish to the public prosecutor upon request all information necessary in accordance with the procedures established by the applicable legislation.

The transmission of information is done by the person designated within the bank's organisation as responsible for reporting money laundering.

Professionals subject to the 2004 Money Laundering Law or their managers or employees may not communicate to the client involved or to any third party that the information has been transmitted to the prosecutor or that an investigation has been started. With the implementation of the Third Money Laundering Directive, the 2004 Money Laundering Law now provides for appropriate exemptions from the tipping off prohibition in particular for banks, insurance companies and other professionals of the financial sector where disclosure is allowed among group members located in the EU or in equivalent third party countries.

In practice, banks are frequently faced with a situation where published information (for example, in newspaper articles) indicates that a client is to some extent involved in a criminal investigation abroad (with often only limited information or details), but

70 EC Directive 2005/60 of 26 October 2005.
71 The full list of underlying offences can be found in CSSF Circular 08/837 (www.cssf.lu).
72 Further guidance on the application of the Luxembourg legislation on money laundering within the financial sector can be found in CSSF Circular 08/387 of 19 December 2008 applicable to all professionals of the financial sector. Following Luxembourg's 2009/10 GAFI audit, a grand-ducal decree was passed on 1 February 2010 which inter alia takes over certain parts of the Circular 08/387 and extents them to all professionals subject to anti money laundering obligations.

where the bank's file on the client and the transactions which were carried out on his accounts have been duly justified and do not show any element which might indicate money laundering. The Luxembourg public prosecutor takes the view that in such case a banker would always be required to denounce his client.

If, however, it is later found that the information was wrong and that indeed the suspicion against the client was unsupported, a declaration by the banker to the prosecutor may have caused serious harm to the client. In order to avoid bankers being reluctant to comply with their denunciation obligation the 2004 Money Laundering Law provides that a good faith disclosure to the public prosecutor by a bank does not constitute a breach of bank secrecy and may not entail any liability on the part of the professional. Such provision is justified in particular in situations where the banker can have legitimate doubts about whether a fact is or is not an indication of money laundering. It is submitted however, that a mere indication of a suspicion of criminal activity published in a newspaper article cannot be by itself an element which is sufficient for the denunciation obligation of the banker to come into existence. The courts have confirmed that such indication in a newspaper, having regard to the information available to the bank, was not in itself sufficient to trigger the requirement for a denunciation.

The banker has thus become subject to a reporting obligation imposed by law and is, in this respect, exempted by law from bank secrecy vis-à-vis the public prosecutor.

Bankers and outsourcing

[26.24] Banks more and more often outsource part of their business to outside professionals. The increased recourse to outsourcing is driven by globalisation, as well as by the requirement to reduce costs in a competitive environment. Bank secrecy has always been a handicap to implementing outsourcing solutions as client data could not be disclosed by Luxembourg bankers. Where Luxembourg banks or professionals of the financial sector took recourse to IT operating systems abroad (which has been an accepted practice within financial groups for many years), the CSSF insisted (absent a specific client consent – see para **[26.25]** below) that any client data be made anonymous which required technically complicated and expensive solutions.

To remedy this situation, the Luxembourg legislator introduced three new categories of professionals of the financial sector by a law of 2 August 2003:

1 'client communication agents', ie professionals in charge of client reporting or of archiving;
2 'financial sector administrative agents', ie professionals who render administrative services to banks, other professionals and investment funds (mainly register and transfer activities, etc); and
3 'operators of financial sector information, technology systems and communication networks', ie professionals in charge of maintaining IT systems or communication networks of banks or professionals of the financial sector.

To the extent that information is communicated to any of these professionals as part of a service contract relating to the activities which are outsourced, the obligation to secrecy imposed by art 41 of the Banking Law does not apply. The exemption introduced in art 41(5) is justified because such professionals are subject to the same bank secrecy provisions, must have a proper organisation allowing compliance with the obligations to which they are subject and are also supervised by the same

These arguments, which are in themselves convincing, have so far not led to any debate on the need for regulation of this subject matter in The Netherlands. The main reason for this is that the current system, based on a contractual general duty to a certain measure eroded by various statutory disclosure obligations, is generally deemed to work satisfactorily both from the banks' and the customers' point of view. In addition, the drafting of a law on this subject will be a complex task, requiring many existing statutory rules in different Acts to be amended; why embark on this if there is no certainty that the result will be any better than the current situation?

THE BANK'S DUTY OF CONFIDENTIALITY

The duty of confidentiality under civil law

[29.2] Under Dutch law, there undoubtedly exists a duty of banks to maintain confidentiality towards their customers. This duty is generally deemed to be based on the contractual relationship between the bank and its customers. This relationship more often than not is governed by the General Banking Conditions 2009 (*Algemene Bankvoorwaarden 2009*) which have been developed by the Dutch Banking Association (*Nederlandse Vereniging van Banken*, or 'NVB') in co-operation with its members and after consultation with consumer representative organisations. Banks in The Netherlands will invariably endeavour to ensure that these General Bank Conditions are part of the contractual relationship. The General Bank Conditions provide in art 2:

> 'The Bank shall exercise due care when providing services. In its provision of services, the Bank shall take the Customer's interests into account to the best of its ability. None of the provisions of these General Banking Conditions or of the special conditions used by the Bank shall detract from this principle.'

The phrases 'to exercise due care' and 'take the Customer's interests into account to the best of its ability' are considered, inter alia, to comprise the duty to maintain customer data confidentiality.

Article 4 of the General Banking Conditions provides:

> 'In providing its services, the Bank does not have to make use of non-public information, including price-sensitive information.'

This proviso is curious; essentially, it relates to the dilemma that a bank may be confronted with when the investment advisory departments of the bank are providing investment advice (or research reports) to its customers whilst in other departments of the bank (for example, the credit department or the corporate finance department) data are available which are confidential but which are certainly relevant to the investment advice to be given or to the contents of research reports that the bank publishes. This problem will be addressed later in this chapter.

The duty of care and the duty to take into consideration the interests of customers would apply to the relationship between a bank and its customers even if they had not been expressed in the General Bank Conditions. These duties are generally considered applicable on the basis of the principle of reasonableness and fairness which is a cornerstone of the Dutch law of contract and, for certain services, on the basis of the bank's duty to exercise the care of a good provider of services (*opdrachtnemer*), including when it acts as a mandatary (*lasthebber*). See arts 6:2, 6:248 and 7:401 of

the Civil Code (*Burgerlijk Wetboek*). The question arises whether the General Bank Conditions, by explicitly referring to this duty of care and this duty to take into consideration the interests of the customers, impose on banks obligations that are more far reaching than the obligations imposed by the principles of reasonableness and fairness of arts 6:2 and 6:248. In Dutch legal doctrine, it is argued that this is indeed the case; however, without specification as to what such extended duty may in practical terms mean.

The General Bank Conditions do not contain any specific provisions on the extent of the duty of confidentiality. Questions such as which data must be kept confidential and which data may without consent of the customer be disclosed must be solved on an ad hoc basis, each time taking into account the specific circumstances in which the question arises. The General Bank Conditions likewise contain no provisions on exceptions to the general principle. Generally, the duty is thought to extend to all data that are not in the public domain. Obviously, where there is a legal duty to disclose (eg on the basis of a statute or by order of a court or supervisory authority), the duty to disclose would generally prevail. By and large banks in The Netherlands are quite meticulous about maintaining the duty of confidentiality, and will tend to seek customer consent whenever banks think this duty may arguably be breached.

Surprisingly perhaps, there is in the Netherlands virtually no case law on the extent of the duty of confidentiality based on art 2 of the General Bank Conditions. This absence of case law appears to indicate that, in practice, few occasions arise where there is a dispute between bank and customer in the application of the duty of confidentiality. A more down to earth reason for the absence of case law may be that the very reason why a customer is interested in a bank's strict adherence to rules of confidentiality often also constitutes a very good reason for that customer not to litigate on the issue.

There is one judgment of the District Court in Zwolle that perhaps deserves to be mentioned here.[1] In this case, the bank had advised a third party of the precarious financial condition of one of its customers. The third party was also doing business with this customer, and providing it with financial facilities. Although it could be argued that it was logical and defensible for the bank to provide information to the third party, particularly given the context of discussions that had been conducted between all parties involved, the bank was nevertheless held liable. The judgment is of a lower court, and therefore perhaps not too much weight should be given to it. Nevertheless, the judgment provides a clear warning that implied consent of a customer should not be easily assumed. Additionally, the judgment seems to indicate also that in (the early stages of) restructuring exercises, especially where lenders are not protected by commonly applicable disclosure provisions in the credit documentation, one should be careful about the exchange of information that is not specifically condoned by the borrower in distress. It should be noted that under certain circumstances the bank's duty of care towards third parties can imply a duty to investigate its own client and potentially notify third parties (further discussed in para **[29.29]** below).

What happens if the General Bank Conditions are not applicable? In certain contractual relations, for example, often in transactions between banks *inter se* and sometimes in transactions between banks and large corporate customers, applicability of the General Bank Conditions is excluded. In addition, it is noted that general conditions that a foreign branch of the Bank applies to its legal relationships with the customer will normally prevail above the General Banking Conditions in the event of a conflict

1 JOR 2000/130, dated 22 December 1999.

Data Protection Directive.[2] In contrast to the confidentiality rules in the financial legislation, as a general rule, the Personal Data Act only applies to information about physical persons.

The current confidentiality provisions were made for a quite different society and today appear not to be well suited in all respects and there is therefore a need for modernising the rules. The Banking Law Commission, a standing governmental appointed banking law committee, delivered on 27 May 2011 a draft proposal for an act consolidating the regulation of financial institutions. *Stortinget* (the Norwegian Parliament) has however not adopted this draft act yet: see 'Proposal for new legislation'.

Personal data rules

[30.2] As mentioned above, the bank confidentiality rules in Norway are directed at the individual officer and employee of the bank and not at the bank itself. Bank confidentiality rules protect all customers, both physical persons and legal entities.

The Personal Data Act implements Council Directive 95/46/EC. The Directive only protects physical persons and the Personal Data Act regulates the collection and treatment of personal information and imposes restrictions on the transfer and disclosure of such information to others. The Act also protects credit information about legal persons.

According to the Personal Data Act, financial institutions are, under certain conditions, allowed to collect and process personal data about customers who are physical persons. Disclosure of such information can only take place to the extent allowed under the Personal Data Act. These restrictions come in addition to restrictions imposed in confidentiality rules elsewhere in the legislation, so that the strictest rule will always apply. The purpose and nature of the personal data rules differ somewhat compared to the confidentiality rules. The proposed legislation attempts to some degree to consolidate the two sets of rules, and corresponding rules with respect to exchange of information within a group are proposed.

To transfer personal data under the Personal Data Act to other entities, the transferring entity must either obtain the relevant person's consent or make use of one of the Personal Data Act's exemptions. If a cross-border transfer is carried out based on these exemptions, the information may as a starting point only be transferred to countries that have adequate regulations for handling personal information. Countries that have implemented Directive 95/46/EC are presupposed to have such an adequate level. If personal information is to be transferred to countries that do not have such adequate requirements, another kind of legal basis, eg acceptance from the person concerned, must be sought.

SCOPE OF BASIC POSITION

[30.3] The present confidentiality rules for banks can be found in the Commercial Bank Act 1961 and the Savings Bank Act 1961. An unofficial translation of section 18 of the Commercial Bank Act (which is similar to the corresponding provision in the Savings Bank Act) reads as follows:

2 Council Directive 95/46/EC.

> 'Elected officers, employees and auditors of a commercial bank are obliged to treat as confidential any information which comes to their knowledge by virtue of their position concerning the bank or a customer thereof, or another bank or its customer, unless they are obliged to disclose information pursuant to this or any other Act. The duty of confidentiality does not apply to information, which the board of directors or anyone authorised by the board discloses on behalf of the bank to another bank.
>
> Notwithstanding this provision, the bank may carry on credit reference activity in accordance with the laws applying thereto.'

In principle, the confidentiality obligations apply to all matters which officers, employees and auditors receive knowledge of in their position in the bank. This includes at the outset 'neutral' information, such as the existence of the customer relationship, name, address, profession etc. 'In connection' means that the person must have received the information in his capacity as employee, officer or auditor, irrespective of whether he actually received the information at the time when he was working. The duty of confidentiality only extends to information which was not publicly known or available at the time. The duty of confidentiality does not extend to matters which are public (other than through illegal disclosure by the bank employee or officer), for instance, through newspapers, television, radio, the Internet or because it is available upon a search of public registers. It would, however, as a main rule be regarded as a breach of the duty of confidentiality for a bank employee to confirm press reports that a given person or entity was a customer, unless the source for such press reports clearly was the customer itself.

The duty of confidentiality extends in principle to any disclosure of such information, including internally within the bank, except that information can be given on a 'need to know' basis. In particular, confidential information cannot freely be given to other legal entities within the same financial group: see 'Information exchange within the group' below.

The confidentiality rules in the Banking Acts do not deal with the question of outsourcing or use of external consultants such as lawyers, etc. In practice, it has been accepted that confidential information can be disclosed to external consultants, but the FSAN stated in a circular of 17 April 2000 that they would regard such consultants as being directly subjected to the confidentiality rules in the Banking Acts. It will be the obligation of the outsourcing entity to ensure that such consultants undertake to keep information received confidential.

Under the rules on securitisation in the Finance Activity Act, financial institutions wishing to assign a loan portfolio to a non-financial institution must notify the borrowers, who must object within a time of not less than three weeks. Under the Financial Contracts Act 1999, a financial institution may transfer a loan to another financial institution without the borrower's consent. The borrower must, however, be notified about the transfer. Neither of these sets of rules authorise the release of confidential information about the borrower(s), and specific consent must therefore be obtained. In the preparation documents for the securitisation rules, the Ministry of Finance expressly states that when the seller is going to act as a service provider/manager of the sold loan portfolio, the seller may not disclose confidential customer information to the purchaser without customer consent, although it is acknowledged that the purchaser may have a legitimate interest in such information. The rules only apply to financial institutions.

The motion referred to in para 1 shall include:

1 the number of the case;
2 a description of the offence being the subject matter of the preparatory proceedings, together with its legal qualification;
3 the circumstances justifying the need to make the information available;
4 an indication of the person or organisational unit concerning the information;
5 the subject obliged to make the information and data available;
6 the type and scope of the information.[60]

Having examined the motion, the court shall, by a ruling, express consent for the information to be made available, specifying its type and scope and the person or organisational unit that it concerns, as well as the subject obliged to make it available, or it shall refuse to grant consent for the information to be made available.[61]

The public prosecutor authorised by the court shall inform in writing the subject obliged to make the information available about the contents of the court's ruling, the person or unit that the information is to concern and the type and scope of such information.[62]

According to art 106c of the Banking Act, the public prosecutor conducting the proceedings in the cases specified in art 105, para 1, subpara 2, (b) and (c) may, on the basis of a ruling issued upon his motion by the locally competent regional court, request the provision of information protected by bank confidentiality by the subjects to which the bank disclosed such information. The provisions of art 106b, paras 2 to 5 shall apply accordingly.

Fiscal incursions into bank confidentiality

[31.33] The wide scope of information, including that of a confidential nature, which is in the banks', insurance undertaking's, investment and pension fund's possession also has to be disclosed to the tax authorities and fiscal control authorities.

Article 105, para 2 of the Banking Act states that the scope of, and the rules concerning, disclosure of information held by banks which is to be disclosed to the tax authorities or fiscal control authorities is regulated by separate legislation. These Acts are the Tax Ordinance Act of 29 August 1997 and the Fiscal Control Act of 28 September 1991. Under these Acts, in certain circumstances, the tax and fiscal control authorities were given almost unlimited access to information possessed by banks about their customers.

Under art 82, para 2 of the Tax Ordinance Act, banks are twice a month (from 1 to 15 of the month and from 16 to the last day of the month) to prepare and provide to tax authorities the information concerning opened and closed bank accounts of undertakings engaged in commercial activity. The information covers the number of the bank account, particulars enabling identification of the holders of such account and the date when the account has been opened or closed.

Banks, insurance undertakings, investment and pension funds are also subject to tax inspections by the tax authorities. The inspectors, to the extent authorised, are entitled, in particular, to request access to records, account books and all documents

60 Banking Act, art 106b, para 2.
61 Banking Act, art 106b, para 3.
62 Banking Act, art 106b, para 5.

connected with the purpose of the inspection and to make copies, extracts, notes, printouts and download data in electronic form.[63]

Under arts 33 and 33a of the Fiscal Control Act, banks are obliged to supply the confidential details of customer accounts upon the written request of the General Inspector of Fiscal Control or a Director of a Fiscal Control Office, but only in the following circumstances:

1 in connection with the preparatory proceedings initiated in a penal case and offence, a fiscal penal case or fiscal offence;[64]
2 in connection with an inspection (initiated by an inspector under issued authorisation) after the prior summons of a taxpayer by the inspector to provide such information or to authorise the financial institutions to pass on the information, but only where a taxpayer:
   (a) has not given consent to the information being disclosed,
   (b) has not authorised the Fiscal Control Office to apply to the financial institution for the information to be passed on, or
   (c) has not, within the time limit specified by the Fiscal Control Office, provided information or authorisation mentioned above, or
   (d) has not delivered the information which is required to be completed or compared with information provided by a financial institution.[65]

The General Inspector of Fiscal Control or a Director of a Fiscal Control Office can request the following information concerning the suspect customer:

1 bank accounts, powers of attorney to manage bank accounts and the amount in such accounts and powers of attorney, as well as their turnover and balance, indicating the inflows and debits of account and their titles and their respective senders and recipients;
2 pecuniary accounts, securities accounts or powers of attorney to manage such accounts and amount in such accounts, as well as their turnover and balance;
3 credit contracts or loan contracts concluded, specifying the amount of the obligations arising from such loans or advances, the purposes for which they have been concluded, and how the repayment is secured, as well as deposit contracts and contracts for provision of safe deposit boxes;
4 state treasury shares or state treasury bonds acquired through banks, as well as trading in these securities;
5 trading in deposit certificates issued by banks or in other securities.[66]

Information listed under points 2 and 4 above may also be respectively requested from other than banks brokerage business operators.

Investment funds are required to prepare and submit information on the date of purchase, number, price and value of the acquired units of participation and the date of repurchase, the number and value of repurchased units of participation, the amount paid to the fund's participant for the repurchased units of participation as well as the date and amount of the fund's incomes paid to the participant, at the written request of the General Inspector of Fiscal Control or the Director of Fiscal Control Office issued in connection with the preparatory proceedings initiated in a penal case and offence, a fiscal penal case or fiscal offence. In the course of the penal or offence proceedings and fiscal penal or offence proceedings by an inspector, control proceedings by a

63 Tax Ordinance Act, art 286, para 1, point 4.
64 Fiscal Control Act, art 33, para 1.
65 Fiscal Control Act, art 33a, para 1.
66 Fiscal Control Act, art 33, para 1.

the purpose of compensating (in part or whole) or otherwise assisting or protecting insured policy owners and beneficiaries under certain circumstances, and for matters connected therewith.

Accordingly, Item 9 has been amended and updated to permit disclosure to lawful recipients for the purposes of complying with the provisions of the Deposit Insurance and Policy Owners' Protection Schemes Act 2011.

Part II, item 1: disclosure in connection with performance of duty

[33.16] As a matter of practice in Singapore, as well as elsewhere, bank officers already often disclose customer information to their colleagues in Singapore, as well as in overseas branches and to their professional advisers. Item 1 has formally recognised this practice as an exception to the duty of bank secrecy.

The scope of the exception is as follows. A bank officer may disclose customer information to his fellow bank officer in Singapore, or to an officer designated in writing by the head office overseas or its parent bank in the case of a foreign-owned bank incorporated in Singapore, in connection with the performance of duty on the part of both parties. The lawful recipient in this case does not however include bank officers from overseas branches and subsidiaries (who have not been so designated by the head office).

Other lawful recipients of such information would be the bank's lawyer, consultant or other professional adviser appointed or engaged by the bank under a contract of service. A further lawful recipient of such information would be an auditor appointed or engaged under a contract of service by the bank, its head office overseas, or its parent bank in the case of a foreign-owned bank incorporated in Singapore.

Part II, item 2: conduct of internal audit and risk management

[33.17] This exception permits disclosure of customer information in connection with the conduct of internal audit or risk management. A foreign bank in Singapore may now disclose to: (i) its head office or parent bank; (ii) an overseas branch designated in writing by the head office; and (iii) a designated 'related corporation' (ie its subsidiaries or affiliates). A local bank may disclose to its parent bank or any related designated corporation. A foreign-owned bank incorporated in Singapore may disclose to its parent bank or any related corporation designated in writing by the parent bank.

Several writers[25] have mentioned the lacuna in the old regime, where disclosure is permitted under the previous s 47(4)(f), to a bank's head office (of information relating to credit/foreign exchange details), under s 47(4)(k) to a bank's local parent bank (of information relating to credit facilities) and s 47(4)(l) to a bank's head office and branch (for the purposes of collating and processing of information). It appeared that while disclosure could be made to a branch of a bank and a parent bank, no disclosure could be made to a subsidiary. Now, at least for the purpose of this exception, a subsidiary can finally be made (by designation) a lawful recipient of customer information.

25 For example Tan Sin Liang 'Banking secrecy – legal implications for banks in Singapore under the Banking (Amendment) Act 2001' [2001] Straits Lawyer, August, at 28.

Part II, item 3: outsourcing operational functions

[33.18] This is a particularly welcome exception which allows a bank to outsource its operational functions and thereby disclose customer information to 'any person including the head office of the bank or any branch thereof outside Singapore' who is engaged to perform the functions.

It has become increasingly more commercially expedient for banks in Singapore to outsource many of their operational functions such as processing of credit cards to third parties, who might enjoy greater economies of scale in that particular function than the banks themselves. This enabled banks to focus on their core banking business in the value chain. However, such activities were not strictly authorised under the former banking secrecy regime – instead, approval from the MAS on a case-by-case basis under the old s 47(12) was necessary before such outsourcing activities could take place. This has now been addressed by the exception in item 3.

The exception draws a distinction between local and domestic outsourcing. If the outsourced function is to be performed outside Singapore, the MAS may impose conditions on the outsourcing contracts, as compared with domestic outsourcing, where no such conditions are imposed. This appears from the parliamentary debate at the second reading of the Banking (Amendment) Bill 2001 to have been done to safeguard against the foreign lawful recipient wrongfully disclosing customer information. However, the deterrent effect against foreign service providers committing an offence under s 47(5) would be open to question, given that the penalties would be difficult to enforce extra-territorially. For that reason, before it would permit a bank in Singapore to disclose customer information overseas, the MAS therefore stipulated a certain level of standing in proposed foreign outsource service providers, and in the legal and regulative framework of its home jurisdiction.[26] Reference should be made to MAS Notice 634[27] to Banks titled 'Banking Secrecy – Conditions for Outsourcing' for conditions to be satisfied if any outsourced function is to be performed outside Singapore. One of the key stipulations of MAS 634 requires banks to notify the MAS of all outsourcing arrangements involving the disclosure and protection of customer information upon entering into the relevant outsourcing agreement outside the jurisdiction.

Part II, item 4 & 4A to 4D: mergers and acquisitions, transfer of business and shares and share capital restructuring

[33.19] This exception permits a bank to disclose customer information in connection with a merger or acquisition, or proposed merger or acquisition, of the bank or its financial holding company, to any person participating or otherwise involved in the merger/acquisition or proposed merger/acquisition (including his lawyers and other advisers), whether or not the merger/acquisition is subsequently entered into or completed.

Obviously, one of the big challenges in the merger or acquisition of a bank is in overcoming the banking secrecy issue. Since not all banks would have provided for a consent to such disclosure in their account opening forms in anticipation of a

26 Parliamentary debates, n 10 above, cols 1709–1710, per the Deputy Prime Minister BG Lee Hsien Loong.

27 19 February 2003, revised on 25 May 2004. For Merchant Banks, see MAS Notice 1108 (19 February 2003, revised on 25 May 2004).

This broad conclusion has been supported since 1978 by the constitutional basis of the principle of bank secrecy. To the extent that the duty of bank confidentiality is connected with the right of privacy of clients as protected by the Spanish Constitution, such right (and the corresponding obligation on the provider of banking services) must be interpreted broadly and may only be limited to the extent that it enters into conflict, or needs to be interpreted in conjunction, with another right protected by the Spanish Constitution and such limits as set out in law. In light of the Constitutional Court's judgment of 26 November 1984, we will analyse the scope of the principle of bank secrecy and in relation to the particular facts subject to revision, namely, the level of information that credit entities are obliged to provide to the tax authorities as regards movements of bank accounts held by clients.

Another specific area of concern is the reports prepared by credit institutions regarding the economic situation of their clients. Although a number of scholars have understood in the past that the principle of secrecy should only cover details regarding particular and usual banking transactions, it seems, taking into consideration the nature of the principle of bank secrecy as a long-standing commercial usage before the enactment of Law 44/2002 and the recognition granted to the principle by the Spanish Constitutional Court as part of the right of Spanish citizens to their privacy, that the release of any report that may serve to identify the client or/and a particular transaction entered into with a credit institution and/or the economic or financial position of the client requires the prior approval of that client. This conclusion is further supported by the fact that the Law 44/2002 regulations that recognise the existence of a duty to keep confidential information regarding clients of a credit entity refer to 'the information relating to balances, operations and any other clients' transactions'.

As regards additional legislation, it is worth mentioning that Royal Legislative Decree 1298/1986 and the Internal Regulations of the Bank of Spain consider privileged information subject to the duty of secrecy to be all the data, documents and information gathered by the Bank of Spain in the performance of the functions vested upon it by existing legislation. Thus, all such information gathered as agent bank to the Spanish Treasury, currency exchange provider and supervisor of the banking system, including, in particular, credit entities, will be subject to the duty of confidentiality.

In the securities market, all information obtained by market participants, including credit entities, in respect of investors, issues and transactions in the market must be kept confidential and safeguarded from improper use as provided for in art 81 of Law 24/1988. In this context, it is important to determine the level of activities and services that credit entities established in Spain (including branches of foreign institutions and EU-based entities under the Second Banking Co-ordination Directive,[4] as implemented in Spain by Law 3/1994) may provide to clients, since information obtained in the provision of those services will be affected by the duty of confidentiality and proper use. In essence, credit entities may perform in Spain all the activities restricted to duly authorised professionals in the securities market (ie investment services companies, namely, securities companies, agencies and portfolio management companies). These include, inter alia:

1 the receipt of orders from clients and their execution or providing for their execution;

4 Council Directive 89/646/EEC.

2 the intermediation in the placement of securities on the account of issuers and their underwriting;
3 the negotiation of securities on their own account;
4 the provision of credit to the market; and
5 the provision of deposit and discretionary portfolio management services to clients.

Below, we will analyse the limits applicable to the principle of bank secrecy affecting its scope. These limits refer, essentially, to the powers of the administrative and judicial authorities to obtain information from credit entities. It is also natural to understand that the scope of the principle of bank secrecy must be limited and constrained by the will of the person or entity protected by it. Thus, if the bank has obtained permission to release any information from the person to whom the information relates, such disclosure must not be deemed in breach of the principle of bank secrecy. This conclusion is contained in Law 44/2002, which, as explained above, exempts from the duty of confidentiality not only the information which must be disclosed by mandate of law or regulatory authority as provided by law, but also the dissemination of information to which the client has consented.

The approval by the affected client as a limit to the principle of bank secrecy was already considered in Royal Legislative Decree 1298/1986. This Decree exempts from the obligation of confidentiality vested on officials of the Bank of Spain that information released with the consent of the affected party. Circular 1/2013 of 24 May of the Bank of Spain, which regulates the central credit risk information-gathering system of the Central Bank, has allowed for information in respect of an individual to be made available to a credit institution with which such client has no contractual relationship, although the client may exercise his/her right to amend or cancel the relevant information should the data be inaccurate or not pertinent. Similarly, the regulations aimed at protecting personal data (specially Organic Law 15/1999 of 13 December on the protection of personal data) provide, when referring to the activity of companies who provide information about the financial position of third parties, that any personal data used in that regard must be obtained from public sources or with the consent of the affected party. In the field of personal data, Organic Law 15/1999 sets out the general rules applicable to the management of data, including communication and storage regulations and rights vested on the holders of the data. In particular, these regulations limit the rendering of outsourcing services to companies which administer personal data by requiring certain minimum contents in the relevant outsourcing agreement aimed at protecting the confidentiality of the data. Additionally, Organic Law 15/1999 limits transfers of personal data to persons or companies located in countries not providing an equivalent protection level to that achieved in Spain, subject to certain exceptions.

The issue of bank confidentiality is also linked to the provision of Internet services by credit entities. The duty to keep confidential all personal data regarding the client is also applicable to these transactions. In this connection, Law 34/2002 of 11 July on information services and electronic commerce, which develops Council Directive 2000/31/EC, sets out the general rules applicable to providers of Internet services located in Spain (information to be displayed on the website, prohibition of unsolicited commercial e-mails, validity of electronic agreements and resolution of disputes, inter alia). This Law will also be generally applicable to providers of Internet services located within the EEA or EU provided that the services relate to specific subjects (such as intellectual property, direct insurance, contracts with natural persons qualifying as consumers, etc).

Public servants such as the members and officers of the FINMA, officers of the Swiss National Bank, tax inspectors, etc are bound by special confidentiality rules governing their respective offices, which involve criminal sanctions as well.[21]

EXCEPTIONS

Customer consent

General

[37.10] Bank confidentiality[22] is not only for the benefit of bank customers in the strict sense, but also for the benefit of third persons who had contacts with customers or about whom the bank obtained confidential information in the ordinary course of its banking business. In order to simplify matters, all those persons are referred to here as 'customers'.

Express or implied consent

[37.11] As the customer is the master of the privileged information, his express or implied consent releases the bank from its confidentiality duty. Since such release must be legally valid, the bank may be in a difficult situation if it has reason to believe that the consent of the customer may not have been given voluntarily, but under material duress originating from a third party, including foreign public authorities. Under the CO, consents given under material duress may be subsequently voided by the customer. Under these circumstances, banks will usually try to obtain clear evidence that the consent expresses the customer's actual intent, for example, by means of prior written consent. Like any communication between the parties to a contract, such a consent will have to be construed in accordance with the 'principle of good faith' established by Swiss jurisprudence. This means communication with the client has to be understood as a reasonable person would have understood it under the given circumstances in good faith.[23] Given the fact that bank confidentiality not only protects a contractual right of the customer, but also his privacy, the test becomes particularly delicate in respect of court-ordered waivers.

Persons acting in lieu of the customer

[37.12] The consent does not need to be given by the customer himself, but may be given by any person authorised under the applicable law to act on behalf of the customer. Thus, consent may also be given by agents or proxies appointed by the customer, legal representatives such as parents, spouses (if applicable), tutors, curators, guardians, officers and directors of a legal entity or successors, heirs and assignees or executors of the customer's will.[24] However, such consent may not be effective if information concerning the customer is of a strictly personal nature. The

21 Cf PC, art 320.
22 In the following sections, the terms 'bank confidentiality' or 'secrecy' and 'bank' also include 'professional secrecy' and 'securities dealer'.
23 Cf BGE 111 (1985) II 276 (279).
24 Aubert et al, n 5 above, pp 299–351.

situation becomes particularly difficult for the bank when the customer is no longer available to clarify inconsistent or partial consent.

As part of the introduction into the CC of new provisions regarding adult protection which came into force on 1 January 2013, the ordinance regarding the asset management in connection with general deputyship or guardianship[25] introduced new disclosure rules for banks. Article 10, sec 3 and 4 of this ordinance provide for an obligation of the bank to disclose bank information to the office of child and adult protection. This disclosure obligation requires, however, a formal decision of the office of child and adult protection.[26]

Justifiable estate of necessity

[37.13] Article 17 of the PC provides that whoever commits an act subject to punishment in order to save his own or third party's legal right from imminent danger that cannot be otherwise averted, is acting lawfully if he is thereby safeguarding higher interests. Such higher interests may include body, life, freedom, honour, property or other essential rights. The concept of justifiable estate of necessity was discussed among Swiss legal scholars in connection with the handing over of client data in the context of threats of foreign governments against Swiss banks. The financial interest of a Swiss bank and its interest to continue its banking operation as well as the protection of bank's employees held in custody by a foreign government have to be balanced against the confidentiality interest of the bank's customer. A balancing of interest has to take into account the specific factual circumstances and may involve difficult questions of judgment. In the UBS case, the Swiss Federal Government has held that the threat of the US authorities to start criminal proceedings against UBS in the United States does not constitute a justifiable estate of necessity pursuant to which UBS could turn over client data to the United States.

The concept of justifiable estate of necessity may also operate as ground for reduction of criminal sanctions. Whoever commits an act subject to punishment to save himself or another from an imminent danger to body, life, freedom, honour, property or other essential rights that cannot otherwise be averted, the judge shall reduce the sentence if the sacrifice of the property could reasonably have been expected from him. If the offender could not reasonably be expected to relinquish the endangered right, he is not acting in a culpable manner (PC, art 18).[27]

Litigation involving the customer

If the customer sues the bank

[37.14] Article 47 of the BkL does not contain an express exception referring to an action by the customer against the bank. However, a customer who sues the bank, but insists that the bank abstains from disclosing facts covered by bank confidentiality when defending its position, acts against the general principle of good faith. Accordingly, banks are entitled to disclose confidential information to the courts

25 RS 211.223.11.
26 Kleiner, Schwob and Winzeler, n 3 above, BkL, art 47, n 76.
27 Kleiner, Schwob and Winzeler, n 3 above, BkL, art 47, nn 326ss; Emmenegger and Zbinden, n 13 above, pp 253s and 270s; P Honegger and A Kolb *Amts- und Rechtshilfe: 10 aktuelle Fragen* in Emmenegger *Cross-Border Banking* (2009) pp 43s; Heine, n 13 above, pp 178s.