Centre for Banking & Finance Law
Faculty of Law

Bank Secrecy Symposium

A Symposium at the Faculty of Law, National University of Singapore, 4-5 December 2014

Report of Proceedings

Editor: Hu Ying

CBFL-Rep-HY1
March 2015

This report may be cited as: Hu Ying (ed), "Bank Secrecy Symposium: Report of Proceedings", Centre for Banking & Finance Law, Faculty of Law, National University of Singapore, March 2015, report number CBFL-Rep-HY1
URL: http://law.nus.edu.sg/cbfl/pdfs/reports/CBFL-Rep-HY1.pdf

ABOUT THE SYMPOSIUM

Most jurisdictions recognise that customer information held by banks should be protected from disclosure to some extent. The boundaries of this protection have shifted in the last decade and more, as the world has intensified its fight against international criminal activity, notably money laundering, terrorism funding and tax evasion. A common feature of the measures taken is an extensive exchange of information regime. Jurisdictions around the world are complying with these unprecedented international pressures to enhance disclosure and afford greater transparency of activities within their borders. Banks are at the centre of the exchange of information initiatives and bank secrecy in many jurisdictions is giving way to these new norms. The symposium will evaluate how bank secrecy in financial centres around the world, from Asia to Europe and the United States of America, is changing.

CHAIR AND CO-CHAIR OF THE SYMPOSIUM

The Symposium was chaired by **Sandra Booysen** (Assistant Professor, National University of Singapore) and co-chaired by **Dora Neo** (Associate Professor and Director, Centre for Banking & Finance Law, National University of Singapore).

SPEAKERS

Sandra Booysen, Assistant Professor, National University of Singapore

Dora Neo, Associate Professor and Director, Centre for Banking & Finance Law, National University of Singapore

Lissa Lamkin Broome, Wells Fargo Professor of Banking Law, University of North Carolina

Stefan Gannon, Executive Director and General Counsel, Hong Kong Monetary Authority

Graham Greenleaf, Professor of Law and Information Systems, University of New South Wales

Christopher Hare, Travers Smith Associate Professor of Corporate and Commercial Law, University of Oxford

Christian Hofmann, Assistant Professor, National University of Singapore

Chizu Nakajima, Professor of Corporate Law and Governance, London Guildhall Faculty of Business and Law

Peter Nobel, Professor, Institute of Law, University of Zurich (Represented by Dr. Beat Braendii)

Stephen Phua, Associate Professor, National University of Singapore

Keith Stanton, Professor of Law, Bristol University

Wang Wei, Associate Professor and Vice-Dean, Fudan University Law School

Masao Yoshimura, Associate Professor, Graduate School of International Corporate Strategy Hitotsubashi University

PERSONAL VIEWS

The views expressed herein are those of the speakers in their private capacities and do not represent the views of their employers.

Centre for Banking & Finance Law
Faculty of Law
National University of Singapore
Eu Tong Sen Building
469G Bukit Timah Road
Singapore 259776
Tel: (65) 6601 3878
Fax: (65) 6779 0979
Email: cbfl@nus.edu.sg

http://law.nus.edu.sg/cbfl/

The Centre for Banking & Finance Law (CBFL) at the Faculty of Law, National University of Singapore, focuses broadly on legal and regulatory issues relating to banking and financial services. It aims to produce research and host events of scholarly value to academics as well as of policy relevance to the banking and financial services community. In particular, CBFL seeks to engage local and international bankers, lawyers, regulators and academics in regular exchanges of ideas and knowledge so as to contribute towards the development of law and regulation in this area, as well as to promote a robust and stable financial sector in Singapore, the region and globally.

National University of Singapore Centre for Banking & Finance Law

Bank Secrecy Symposium

4-5 December 2014

Report of Proceedings

Convened by:

Sandra Booysen

Assistant Professor, National University of Singapore

and

Dora Neo

Associate Professor and Director, Centre for Banking & Finance Law, National University of Singapore

Table of Contents

INTRODUCTION

On 4-5 December 2014, the Centre for Banking & Finance Law at the National University of Singapore held a Bank Secrecy Symposium (the "Symposium"). The Symposium brought together speakers, commentators and observers from academia, financial regulators, banks and law firms to discuss theoretical and practical issues that arise in bank secrecy laws in financial centres around the world. The Symposium addressed a range of issues including the conceptual basis for bank secrecy obligations, conflicts of law issues associated with bank secrecy, substantive bank secrecy rules in various jurisdictions, and the relationship between bank secrecy and other laws including data protection legislation as well as anti-money laundering (AML), counter-terrorism financing (CTF) and anti-tax evasion regulations.

The Symposium proceedings were divided into two parts. The first part consisted of five presentations, which examined issues of general importance to bank secrecy laws. The second part of the Symposium consisted of eight country-specific presentations, which provided an in-depth overview of the bank secrecy laws in China, Germany, Hong Kong, Japan, Singapore, Switzerland, the United Kingdom (UK) and the United States (US). Parts one and two of this report summarise the key issues covered in the papers presented at the Symposium; part three highlights the main comments and observations made during the follow-up discussions.

PART ONE: GENERAL ISSUES

I. A Conceptual Overview of Bank Secrecy[1]

Dora NEO, Associate Professor, National University of Singapore

Banks in many countries have a legal obligation to keep customer information secret. This obligation may arise by way of a statute, contract, or a combination of both.

Prima facie, there are different rationales for the establishment of bank secrecy laws. For countries which enact statutes providing generally for professional secrecy, the predominant aim is likely to be the protection of privacy and confidentiality.[2] Other countries may enact specific bank secrecy statutes for pragmatic reasons: strong bank secrecy laws tend to attract foreign banking business and in turn enhance the competiveness of a country's banking sector and support its growth as a financial centre. Moreover, the bank secrecy obligation sometimes arises in contract, usually by way of an implied term in the contract between the bank and its customers. The leading UK case on this point is *Tournier v National Provincial and Union Bank of England* ("*Tournier*").[3] The implied term approach taken in *Tournier* and similar cases gives primacy to the contractual intention and expectations of the parties to the banking relationship, which form the basis of the bank secrecy obligation.

Amongst various rationales, privacy and confidentiality are arguably the most important underlying concepts for bank secrecy. Both pragmatic and contractual bases for bank secrecy can ultimately be tied back to concerns of privacy and confidentiality. Where pragmatism leans in favour of protecting bank secrecy for economic growth, this is because of the value that individuals attach to privacy and confidentiality. In the case of implied terms, the basis for the bank's duty of secrecy is contractual; but the reason that

[1] The report of this presentation is based on Professor Neo's presentation at the Symposium.
[2] Confidentiality overlaps with privacy but is not identical to it. Privacy rights are more fundamental in that they precede the obligations of confidentiality. As R Pattenden has put it, "confidentiality requires some privacy, privacy requires no confidentiality".
[3] [1924] 1 KB 461.

makes it necessary to imply this term is to give effect to the confidential relationship between the customer and the bank.

Bank secrecy laws are more widely accepted than general privacy laws. Many jurisdictions recognise a duty of bank secrecy but not a general right of privacy. Furthermore, recent developments in bank secrecy and privacy laws have taken different paths. Developments in relation to bank secrecy laws have been largely to curtail its scope and to allow or require banks to disclose customer information in an increasing number of situations. The reasons for such curtailment include the rise of terrorism, money laundering, the increased determination of governments to crack down on tax evasion, and new ways of conducting business such as by outsourcing (which require banks to disclose customer information in wider circumstances). By contrast, technological advancement and social change have resulted in proliferation of laws protecting the right to privacy. Major developments in privacy laws include the recognition of respect for private and family life in the European Convention on Human Rights, and the widespread enactment of data protection legislation worldwide.

II. Conflicts of Laws, Bank Secrecy and the Death of Branch Banking[4]

Christopher Hare, Travers Smith Associate Professor of Corporate and Commercial Law, University of Oxford

The conflicts of law problems associated with the bank's duty of secrecy arise from the following key factors:

1. The default rule in many jurisdictions allowing the courts to exercise jurisdiction over a bank solely based on the establishment of a branch of that bank within the jurisdiction;

2. The fact that many banks have extensive overseas branches which are generally

[4] The report of this presentation is based on Professor Hare's presentation at the Symposium.

treated as part of one corporate entity; and

3. The different scope of bank secrecy obligations (whether founded in statute or contract) in different jurisdictions.

These factors have resulted in the ability of persons seeking disclosure orders against the bank to forum shop for the jurisdiction affording them the widest disclosure rights. This has in turn resulted in cases where banks are faced with the choice of complying with a court order made in jurisdiction A to disclose information or comply with bank secrecy laws in jurisdiction B which makes the same disclosure a breach of bank secrecy. In presenting the issues above, the paper examined the basis for the exercise of jurisdiction against banks both under common law and in accordance with the Brussels I Convention between European Union members.

The applicable law governing a bank's obligation to keep customer information secret depends upon the source of that obligation and its characteristics for choice of law purposes.

Where the bank secrecy duty has statutory origin, its international reach is determined by the territorial application of the relevant legislation. Significantly, most courts would likely refuse to give effect to national legislation of another country purporting to have international effect as it would be tantamount to the direct or indirect enforcement of a foreign penal or "other public law".[5] Furthermore, even the courts of the relevant country may be inclined to read the legislation as only applying within the jurisdiction unless it is clear from the language that extra territorial effect is intended.

Where bank secrecy obligations are founded on contract, different considerations apply.[6] In such cases, the existing default rule stipulates that the governing law is that of the place of the branch where the relevant account is set up.[7] However, the primary

[5] See, e.g., *QRS 1 ApS v Frandsen* [1999] 1 WLR 2169, 2171.
[6] As concerns regarding extra territoriality and penal legislation become less important.
[7] See, e.g., *Libyan Arab Foreign Bank v Bankers Trust Co*, [1989] QB 728, 746.

justifications for the default branch rule are not as convincing as they might once have been. To begin with, this rule relies upon the notion of legal separation between a bank's various branches and its head office, a notion which has been gradually eroded.[8] Moreover, this rule is based upon the notion that demand and repayment must be made at the particular branch where the account is kept, which notion is increasingly at odds with modern banking practice.[9] Further, to the extent that this rule was based upon customer expectations regarding how their dealings with the bank are to be governed, that rule no longer represents what a modern customer expects of his bank. There are additional reasons which make it inappropriate to apply the default rule to the bank's contractual duty of secrecy to its customers: Firstly, where a customer deals with a bank by phone, the call center employees will access the customer's bank information in a jurisdiction (frequently India) that is far removed from the bank's head office or branches. Secondly, no matter how the customer accesses his information, the reality is that customer information is no longer recorded in bank ledgers that are held at a particular branch, but is instead stored electronically.

In light of the above, it is time to revisit this over-reliance on the notion of the branch as the basis for applying conflicts of law principles.

III. The International Pressures on Banks to Disclose Information

[8] In *Walsh v National Irish Bank Ltd* [2013] IESC 2, [5.6], the Irish Supreme Court made clear that the courts would only maintain the distinction when it was appropriate to do so.

[9] Demand is not necessary in relation to all types of account. Moreover, the requirement that a demand for repayment must be made at the branch where the account is kept is nowadays often overridden by contrary agreement.

– The Development of Anti-Money Laundering and Counter Terrorist Financing Regimes and the Conflicting Demands in the Global Setting[10]

Chizu Nakajima, Professor of Corporate Law and Governance, London Guildhall Faculty of Business and Law

The Financial Action Task Force (FATF), established in June 1989 at the Economic Summit of the Group of Seven, has become the international standard setter in the global fight against money laundering and terrorist financing.[11] In April 1990, the FATF announced forty recommendations on money laundering for its member counties. Recommendation 16 introduced the notion of suspicion-based reporting by financial institutions to the competent authority. The forty recommendations were updated in 2012. Recommendation 29 now requires each country to establish a financial intelligence unit (FIU) that serves as the national centre for the receipt and analysis of suspicious transaction reports and other information relevant to prohibited activities, e.g., money laundering and terrorist financing.

Two of the 2012 recommendations directly address bank secrecy:

1. Recommendation 9 requests member countries to ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

2. Recommendation 21 (a) requests member countries to protect financial institutions, their directors and officers from criminal and civil liability for reporting suspicious activities in good faith to the FIU.

The FATF has developed an assessment mechanism based on mutual evaluation to ensure that jurisdictions comply with the FATF recommendations that they have endorsed. The most recent round of mutual evaluation began in 2014. The FATF has used a "carrot and stick" method to induce and coerce countries into implementing its

[10] The report of this presentation is based on Professor Nakajima's presentation at the Symposium.
[11] The FATF's mandate expanded beyond AML in 2001 to CTF and in 2008 to combat the proliferation of weapons of mass destruction.

recommendations. The carrot is offered by the World Bank and the International Monetary Fund through the provision of technical assistance and the increased incorporation of AML/CTF assessment into loan/development packages.[12] The stick is delivered through naming and shaming those jurisdictions which deemed by FATF to lack adequate AML measures, e.g., listing them as Non-Cooperative Countries and Territories.

Banks owe conflicting duties to keep their customer information secret and to disclose customer information to national authorities, such as FIUs. Although AML/CTF related laws may protect banks from liability resulting directly from disclosure to competent authorities, banks may still be exposed to other liabilities, e.g., when they disclose information to third parties.

Many countries are under pressure to gain "legitimacy" in the international arena by adopting transparency measures in areas such as AML, CTF and tax evasion. The global trend toward greater transparency seems difficult to reverse. However, there arguably should be more discussions on the limit of the international drive for transparency and the appropriateness of turning commercial entities such as banks into reluctant policemen.

IV. Convergence in Global Tax Compliance[13]

Stephen Phua, Associate Professor, National University of Singapore

Reducing public funding gaps is a big challenge for many countries. As the tools and policy options for comprehensive tax reforms are limited, it is submitted that nations should consider allocating more resources to review their tax gaps, i.e., the difference between the full potential tax revenues legally due to the state and the actual amount

[12] O. Bures, *EU Counterterrorism Policy: A Paper Tiger*? (2011) Ashgate, Farnahm, at 178.
[13] The report of this presentation is based on Professor Phua's presentation at the Symposium.

of tax collected. Studies have shown an average tax gap of about 14%, 13% and 9% respectively in Australia, the United Kingdom and the United States.[14] Tax gaps in selected developing countries are much higher: in Bangladesh, South Africa and Thailand, the average tax gaps are about 36%, 23% and 53% respectively.[15]

The principal cause of non-compliance with tax laws is information deficiency. Recent domestic tax reforms in developed economies have sought to reduce information deficiency in several ways:

1. Enhancing accounting disclosure standards: The United States Financial Accounting Standards Board released FIN 48 (FASB Interpretation 48) which clarified how Uncertain Tax Positions (UTP) are to be treated in businesses' financial statements.

2. Expanding information reporting obligations:

    a. The United States Inland Revenue Service (IRS) requires certain corporations to disclose some of the information relating to UTPs directly to the tax authority.[16] A similar regime was recently adopted in Australia.[17] The UTP disclosure regime is highly desirable from the tax authority point of view as it promotes and fosters disclosures vital to self-assessment systems. However, it is also both coercive and controversial. Doubts have been cast on the legality of IRS's attempt to rely on its power to require people to file tax returns to support the demand for disclosure; some of the disclosures may potentially conflict with the protection conferred on certain confidential information.

---

[14] Friedrich Schneider, "Shadow Economies around the World: What do we really know?" European Journal of Political Economy, Volume 21 Issue 3 (Sept. 2005) 598-642.
[15] *Ibid*.
[16] As at 2014, corporations with assets in excess of 10 million USD are required to comply with the UTP disclosure. See IRS 2012 Instructions for Schedule UTP (Form 1120), <http://www.irs.gov/pub/irs-pdf/i1120utp.pdf>; IRS Announcement 2010-75 "Reporting for Uncertain Tax Positions," p 4.
[17] There is no specific legislation that mandates this disclosure. The power to demand the submission is apparently derived from ss 161 and 161A of the Australian Income Tax Assessment Act 1936 that requires the income return to be submitted in an approved form.

b. Moreover, the IRS has implemented new measures to improve third party reporting, e.g., from 2011, organisations that process credit and debit card payments must submit annual reports of these payments to the IRS.[18] Similar third-party reporting obligations have been implemented in countries such as Japan[19] and Ireland.[20] Jurisdictions such as Canada, Norway and the UK impose reporting requirements specifically on the building and construction sectors.[21]

3. Whistleblowing programs: various countries have implemented whistleblowing programs to bridge information asymmetry. However, they generally face two obstacles: first, potential whistleblowers do not want to risk self-incrimination; second, confidentiality undertakings by the tax administration are perceived to be inadequate.

At international level, there has been greater cooperation between tax authorities worldwide through the widespread adoption of The Organisation for Economic Cooperation and Development (OECD) standards on international exchange of information[22] and bilateral withholding tax agreements.[23] Apart from encouraging foreign authorities to disclose information, the US has taken the more controversial approach of imposing contractual obligations on foreign financial institutions to report information about financial accounts held by US taxpayers to the IRS and withholding

[18] Inland Revenue Code (Title 26), §6050W; Housing Act 2008, §3091(a).
[19] For Japan, see The Organisation for Economic Cooperation and Development (OECD), "Information Note: Withholding & Information Reporting Regimes for Small/Medium-sized Businesses & Self-Employed Taxpayers, 2009, Annex 1, pp 45-46, 57.
[20] For Ireland, businesses, professionals or other non-profit making organisations are required to report details of any payment exceeding €6,000 for certain types of services rendered. This is known as "Third Party Returns". The categories of services that fall within this scheme include entertainment, merchandising and photography.
[21] For Canada, see the "Contract Payment Reporting System", <http://www.cra-arc.gc.ca/nwsrm/fctshts/1999/m12/cnfct-eng.html>. For Norway, see OECD, "Information Note: Withholding & Information Reporting Regimes for Small/Medium-sized Businesses & Self-Employed Taxpayers", 2009, Annex 1, pp 52-53. For the UK, see the "Construction Industry Scheme", <www.hmrc.gov.uk/cis/>.
[22] The Global Forum on Transparency and Exchange of Information for Tax Purposes, Information Brief (10 August 2011), Annex III, p 13.
[23] See, e.g., the agreements concluded between Switzerland and several European countries (e.g., Germany and UK) to withhold taxes on future investment income and capital gains of residents in those countries.

tax at 30% on any payment of taxable US income to a non-participating foreign financial institution (See the Foreign Account Tax Compliance Act (FATCA) 2010).[24]

The paper also briefly discussed the effectiveness of various types of penalties in promoting compliance with tax laws. It concluded by identifying the challenges to reducing tax gaps in developing countries and argued that reforms in these countries should focus on improving their tax administration.

V. Banking and Data Privacy Legislation: International Trends, Asian Comparisons[25]

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales

Data privacy laws have spread worldwide at an accelerating speed since the first such law in 1973. As at December 2014, 109 jurisdictions have data privacy laws; it is the first time that the majority of global privacy laws are from outside Europe.

Three generations of data privacy principles have been identified:

1. the "minimum" data privacy principles of the early 1980s:[26]

2. the "European" principles; [27] and

[24] Note that a number of countries have signed inter-governmental agreements with the United States, which require the non-participating foreign financial institutions (FFIs) in those countries to identify US taxpayers holding accounts in these FFIs and to report information about these accounts to the US.

[25] The report of this presentation is based on Professor Greenleaf's presentation at the Symposium.

[26] These principles are enshrined in (1) the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted on 23 September 1980 and (2) the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I. 1981 (the "CoE Convention").

[27] These principles are embodied in (1) the European Communities Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement

3. the post-2015 new European principles.[28]

Twelve Asian jurisdictions have significant data privacy laws affecting their private sectors. Six of these laws are comprehensive, covering both the public and private sectors: Hong Kong,[29] Japan,[30] South Korea,[31] Macau,[32] the Philippines[33] (not yet in force), and Taiwan.[34] Three others cover most of the private sector (India,[35] Malaysia,[36] and Singapore[37]), and a further three (China,[38] Vietnam,[39] and Indonesia[40]) have data privacy laws which only cover their e-commerce and consumer sectors. Data protection laws in these Asian jurisdictions are midway between the "minimum" and "European" principles.

Moreover, the obligations imposed by data privacy laws, while often in parallel with traditional duties on banks, are generally much broader in scope and hence require new accommodation in the banking industry:

1. Personal data v. customers: all Asian data privacy laws protect personal data, which is essentially any data with the capacity to identify a person (not actual identification). The type of information protected under data privacy laws is arguably wider than that traditionally protected by the banks' duty of secrecy.

---

of such Data, adopted on 24 October 1995 and (2) some additional elements found in the CoE Convention and its 2001 Additional Protocol (Strasbourg, 8.XI.2001).

[28] Proposals to reform the data protection laws in Europe will probably finalise in 2015.

[29] Personal Data (Privacy) Ordinance 1995 (Hong Kong SAR).

[30] Act on the Protection of Personal Information 2003 (Japan) and related legislation.

[31] Personal Information Protection Act 2011 (South Korea).

[32] Personal Data Protection Act 2005 (Macau SAR).

[33] Data Privacy Act 2012 (Philippines).

[34] Personal Data Protection Act 2010 (Taiwan).

[35] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India).

[36] Personal Data Protection Act 2010 (Malaysia).

[37] Personal Data Protection Act 2012 (Singapore).

[38] Standing Committee of the National People's Congress (SCNPC) Decision on Internet Information Protection 2012 (China), SCNPC Amendments to the Consumer Law 2013 (China), and subsidiary legislation.

[39] Law on Information Technology 2006 (Vietnam).

[40] Regulation on the Operation of Electronic Systems and Transactions 2012 (Indonesia).

2. Minimum collection v. know your customer: the majority of Asian data privacy laws adopt the stricter "European" approach of "minimum" collection, i.e., personal data should only be collected where it is necessary for a (legitimate) specified purpose. In contrast, banks may be required by AML/CFT legislation to conduct extensive "know your client" checks, the scope of which might go beyond what data privacy laws would justify.

3. User/disclosure restrictions v. *Tournier* exceptions: all Asian data protection laws require personal data to be used and disclosed only for the purpose for which it is collected (with limited exceptions). The requirements are arguably more restrictive than the principles enunciated in *Tournier*, which for example allow banks to use customer information internally.

4. Security and data breach: all Asian jurisdictions require personal data to be protected by reasonable security measures. The standard of care required under such measures is sometimes higher than that required under the bank's duty of secrecy to protect customer data.

5. Access, correction and other new customer rights: data privacy laws in Asian jurisdictions (except China) provide for some minimum user access and correction rights. In this respect, data privacy laws are wider in scope than bank secrecy laws since the latter are less concerned with protecting people's right to access or correct their information.

PART TWO: COUNTRY-SPECIFIC REPORTS

VI. Bank Secrecy in China[41]

Wang Wei, Associate Professor, Fudan University Law School

China's protection of bank secrecy is weak. It has not enacted any formal privacy law for individuals or institutions, and has no legislative plans to do so. The existing rules which govern bank secrecy are far from coherent and seldom enforced. By contrast, the powers by various government authorities to request information from financial institutions are more extensive and real.

The bank's duty of secrecy towards their customers can be found in only a few laws and regulations:

1. The Administrative Regulation on Savings:[42] Article 32 provides that savings institutions have a duty of secrecy towards their depositors.

2. The General Rules on Lending:[43] Paragraph 4 of Article 23 states that lenders have a duty of secrecy in respect of their borrowers' debts, financial information, production and operations.

3. The Commercial Banking Law:[44] Articles 29 and 30 provide that commercial banks have a *right* to refuse requests from any institution or individual to enquire about, freeze or deduct any savings account. Notably, these provisions use the term "right", rather than "duty" to describe the bank's obligation.

4. The Chinese Contract Law:[45] Articles 43 provides that a person may not disclose or improperly use trade secrets acquired in the course of negotiating a contract. Article 60 provides for a general duty of secrecy, the scope of which is determined in light

[41] The report of this presentation is based on Professor Wang's presentation at the Symposium.
[42] Published by the State Council in 1992 and amended in 2010.
[43] Published by the People's Bank of China in 1996.
[44] Enacted by the National People's Congress in 1995 and amended in 2003.
[45] Enacted by the National People's Congress in 1999.

of the nature and purpose of the relevant contract as well as customs of trade. In a contractual dispute on a savings deposit, the Shanghai No.1 Intermediate People's Court of Shanghai held that the bank's duty of secrecy towards depositors is an important contractual obligation.[46] This contractual duty is bilateral, not unilateral. For example, in a recent case, a customer's bank card was cloned and the fraudster withdrew money using the fake card and the correct password. The customer sued the bank to recover his losses. The Guangdong Higher People's Court held that, while the bank's failure to spot the fake card was the main cause of the customer's loss, the customer also owed a duty to safeguard his password from unauthorised use and breached his duty. Hence the bank was held 70% liable.[47]

However, the bank's duty of secrecy is not absolute. Exceptions to that duty can be found in a number of laws and rules, including, for example, Article 242 of the Chinese Civil Procedure Law, Article 142 of the Chinese Criminal Procedure Law, paragraph 6 of Article 54 of the Chinese Tax Collection Law, and paragraph 5 of Article 6 of the Chinese Customs Law. Of particular relevance is the Administrative Rules for Financial Institutions to Assist the Work of Inquiry, Freezing and Appropriation[48] issued by the People's Bank of China in 2002. Under these Rules, an extensive list of competent authorities may request information from financial institutions, including (1) the people's courts; (2) tax authorities; (3) customs; (4) people's procuratorates; (5) public security authorities; (6) national security authorities; (7) military guard authorities; (8) prisons; (9) investigation authorities for smuggling; (10) supervisory authorities; (11) auditing authorities; (12) administrative authorities for industry and commerce; and (13) regulatory authorities for securities.

[46] *Luomou v. Yi Bank, et. al.*, (2011) *huyizhong minliu (shang) zhongzi* No. 198. The judgment was delivered on 3 February 2012.
[47] *Dinghuogui v. Agriculture Bank of China Sihui Bihaiwan Sub-branch*, (2013) *Yuegaofa miner tizi* No. 19. The judgment was delivered on 28 February 2014.
[48] Yinfa (2002) No.1, issued on 15 January 2002 by the People's Bank of China.

VII. Bank Secrecy in Germany[49]

Christian Hofmann, Assistant Professor, National University of Singapore

Germany does not have any statutory provisions on bank secrecy, but it is widely acknowledged that customers have a contractual right against their banks to have information arising from their relationship kept confidential. All information obtained during the contractual and in the pre-contractual stage is covered by bank confidentiality. The entire bank is subject to the obligation of secrecy and internal dissemination of confidential information, e.g., through a data sharing system, is restricted. The obligation of secrecy extends to banks that have been granted access to customer information held by other banks. In addition to contractual principles, customer information is further protected by data privacy laws.

Customer consent is generally required if banks wish to disclose customer information to private entities. Consent may be explicit or implied. If there is no time to seek prior consent from a customer, a bank may disclose that customer's information if it has good reasons to conclude that sharing such information is in the customer's best interest. Transfer of customer data to the credit rating agency SCHUFA[50] is further regulated by section 28a of the Federal Data Protection Act. This provision seeks to protect natural persons – creditors are not permitted to disclose sensitive information referring to natural persons unless the requirements set out in section 28a are satisfied.

In contrast, extensive exemptions exist under German law to enable public authorities, in particular, financial regulators and tax authorities, to access confidential information held by banks.[51]

---

[49] The report of this presentation is based on Professor Hofmann's presentation at the Symposium.
[50] SCHUFA stands for Schutzgemeinschaft Für Allgemeine Kreditsicherung.
[51] Limited protection for banks and their customers is provided by the Constitution (e.g., Article 2(1) of the Constitution guarantees every person the right to self-determination in matters of privacy) and certain statutory provisions, e.g., s.9 of the Banking Act imposes confidentiality obligations on the bank's supervisory bodies. These obligations generally prevent national supervisors from sharing

1. Financial regulators: Section 44 of the Banking Act requires banks and several other types of financial institutions to provide requested information to supervisory authorities, i.e., the federal agency for supervision of financial services (Bundesanstalt für Finanzdienstleistungsaufsicht, or BaFin for short) and the German central bank. The most intrusive effect for bank customers stems from section 24c(1) of the Banking Act which requires all supervised institutions to keep and update lists with the name and date of birth of every account holder, their account numbers and the dates when the accounts were opened and closed. The supervisory authorities may access this database to perform their prudential tasks under the Banking Act or the Money Laundering Act. The only additional and, to some extent, restrictive requirement is that access must stem from "particular urgency in individual cases." Worse still, data access takes place in secret. Section 24c(1) further requires the bank to ensure that the BaFin has automated access at all times and that such access goes unnoticed by the bank. The secrecy makes it extremely difficult for affected bank customers to assess whether the conditions for data access have been complied with.

2. Tax authorities: Tax authorities also have power to bypass the customer and request information directly from the bank. Under section 97 of the General Fiscal Code, tax authorities may request that banks present account records and other documents for inspection and examination. The authorities must indicate whether they seek such information in order to tax the bank or its customers, and they may only require the bank to provide documents if the relevant customer has failed to furnish them, or has provided insufficient or (potentially) incorrect information.[52] Tax authorities also have access to data that banks are required by section 24c of the Banking Act to keep and update (see paragraph 1 above). However, such access is more restricted than that for the financial regulators. For example, the tax

information with their counterparts from countries that do not observe similar confidentiality requirements.

[52] S97(2) of the General Fiscal Code.

authorities must first seek to obtain the information from the bank customer directly and must inform the affected customer of the disclosure.[53]

In conclusion, the bank secrecy principles provide relatively strong protection for disclosure of information by banks to private entities. However, the protection provided for disclosure of information to the state is feeble.

VIII. Bank Secrecy in Switzerland[54]

Peter Nobel, Professor, University of Zurich, presented by Dr. Beat Braendii

Paragraph 47 of the Swiss Banking Act makes it a criminal offence for persons to deliberately disclose "confidential information entrusted to them in their capacity as a member of an executive or supervisory body, employee, representative, or liquidator of a bank". A few basic principles relating to bank secrecy under Swiss law are set out below:

1. The Swiss law has been in line with the FATF recommendations and bank secrecy is not a defence for the transfer of information on money laundering issues.

2. Swiss banks are not allowed to rely on bank secrecy principles to deny the supervisory authority access to their information.[55] Foreign banks are also allowed to provide their home regulators with necessary information.[56]

3. The banks' general terms and conditions have traditionally been silent on matters of bank secrecy. Recently, new provisions have been included to obtain consent from customers to waive the bank's duty of confidentiality under certain circumstances.

---

[53] See the „ Anwendungsrelass zur Abgabenordnung – Regelungen zu §§ 92 und 93 AO", Gz. IV A 4-S 0062-1/0 of 10 March 2005; P. Schantz, in: Schwintowski, Bankrecht, 4th ed. 2014, 51, 64 seq.
[54] The report of this presentation is based on Professor Nobel's paper, presented by Dr. Braendii at the Symposium.
[55] See, e.g., paragraph 29 of the Financial Market Supervision Act.
[56] Article 4 quinquies of the Banking Act.

4. The Swiss Federal Court has always been of the opinion that bank secrecy is not a constitutional right. However, it is uncertain whether bank secrecy will have a constitutional basis following the popular initiative "Ja zum Schutz der Privatsphäre" (Yes to the protection of privacy), which was launched in May 2013 to protect bank secrecy.

5. The right to refuse to give evidence based on bank secrecy can only be exercised where the interest of secrecy outweighs the interest of establishing the truth.[57] This requirement is rarely satisfied.

Switzerland makes a distinction between tax evasion and tax fraud. Tax evasion means the non-declaration of funds, whereas tax fraud signifies an active deception such as lying or using false documents to deceive authorities. Only tax fraud constitutes a criminal offence. Hence, Switzerland traditionally refused judicial and administrative cooperation in respect of tax evasion.

However, recent international initiatives to facilitate disclosure and exchange of information have lead Switzerland to adopt a more cooperative approach in tax matters. For example, Switzerland has concluded a number of bilateral treaties on withholding tax with countries such as the US,[58] UK[59] and Austria.[60] It has also withdrawn its reservations to the OECD Model Tax Convention on Income and on Capital concerning exchange of information in tax matters in 2009 and has implemented measures to facilitate group administrative assistance requests from other jurisdictions.[61] After a series of high profile legal proceedings brought in the US against Swiss banks such as

[57] Article 166, Part II of the Swiss Code of Civil Procedure; Article 173, Part II of the Swiss Criminal Procedure Code.
[58] E.g., to facilitate the implementation of the Foreign Account Tax Compliance Act (FATCA).
[59] Agreement between Switzerland and the United Kingdom of Great Britain and Northern Ireland regarding the Collaboration in Tax Matters, concluded on 6 October 2011, with a protocol for further amendments from 20 March 2012, in force since January 1st 2013, SR 0.672.936.74.
[60] Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Republik Österreich über die Zusammenarbeit in den Bereich Steuern und Finanzmarkt, concluded on 13 April 2012, in force since 1 January 2013, SR 0.672.916.33.
[61] See the Federal Act on International Administrative Assistance in Tax Matters of 29 September 2012, SR 672.5.

UBS and Credit Suisse, the Swiss government has further issued a joint statement with the US to allow banks to participate in a unilateral programme of the US Department of Justice to rectify their past wrongdoings.[62]

IX. Bank Secrecy in Japan[63]

Masao Yoshimura, Associate Professor, Hitotsubashi University.

Japan does not have any statutory provision on bank secrecy. Protection of customer information is provided for by the customs of merchants, contract law, and, more recently, under general legislation such as the Data Protection Act.

Changes in Japan's economic and political policy have played a crucial role in shaping Japan's law on bank secrecy as well as exchange of information in tax and other matters. During and after the World War II, the Japanese government strongly encouraged savings. Customers were allowed to hold anonymous bank accounts and had no obligation to file tax returns for the interests they received. As a result, protection of bank secrecy or tax evasion was not a major concern.

As Japan's economy gradually recovered from the war, the government started to charge withholding tax and the National Tax Agency concluded an agreement with the Japanese Bankers Association in 1950 which required banks to disclose certain customer information to facilitate tax investigation. In 1979, the government proposed to introduce a "Green Card" system to change its pro-savings policy. The proposal, which involved issuance of a green card to each bank customer who held a tax-free savings account, was not well-received and was abandoned in 1985. The government subsequently introduced a 20% flat rate withholding tax and abolished tax-free savings

[62] Joint Statement between the US Department of Justice and the Swiss Federal Department of Finance, signed on 29 August 2013, <www.efd.admin.ch>.
[63] The report of this presentation is based on Professor Yoshimura's presentation at the Symposium.

accounts. Since 1996, Japan has undertaken significant financial reforms to develop its economy and to encourage investment in the financial market.

As Japan moved away from a pro-saving to a pro-investment policy, it has also enacted various laws to protect personal data and to prevent money laundering and tax evasion. In 2003, Japan enacted the Act on the Protection of Personal Information, which provided data protection rules for businesses, including financial services. The Act is supplemented by more detailed guidelines issued by the Financial Services Agency (FSA). The guidelines provide that financial institutions:

1. cannot in principle acquire sensitive information (such as political positions, religious and ethnic information, and place of birth) from their customers;

2. cannot share their customers' personal data with third parties without the customers' written consent; and

3. shall notify the FSA and their customers if there is a leakage of customer personal data.

Japan has developed AML regulations to implement FATF's recommendations and supports international disclosure of information in tax matters: it has signed several tax treaties and agreements with countries such as the US.[64] One recent measure introduced by the Japanese government to prevent tax evasion is to require the use of a Social Security and Taxpayer Identification Number for opening of bank accounts and other purposes.

[64] Japan has concluded an agreement with the US to implement the Foreign Account Tax Compliance Act (FATCA) and has opted for the FATCA model 2 agreement.

X. Bank Secrecy in the United Kingdom[65]

Keith Stanton, Professor of Law, Bristol University.

UK does not have any statutory provision on bank secrecy, but the bank's obligation to keep customer information secret is well-established. A number of legal principles support this obligation:

1. Contractual duty: *Tournier* recognises the duty of secrecy as an implied contractual obligation owed by a bank to its customers. The duty is not absolute. *Tournier* has identified four qualifications to that duty: "(a) where disclosure is under compulsion by law; (b) where there is a duty to the public to disclose; (c) where the interests of the bank require disclosure; (d) where the disclosure is made by the express or implied consent of the customer".[66]

2. Agency principles: The banker/customer relationship is, in some respects, an agency relationship and agents owe a duty of confidentiality with regard to their principals' affairs.

3. Voluntary Codes: the *Tournier* principles were reproduced in the voluntary code of practice adopted by the UK banking industry until 2009. The code was not legally binding, but may be taken into account when assessing whether a bank had acted reasonably. The code has subsequently been replaced by direct regulation (see paragraph 4 below).

4. Financial Services and Markets Act 2000 (the "FSMA"): Under FSMA, banks are regulated by the Prudential Regulation Authority and the Financial Conduct Authority. The regulation is effected by means of handbooks which are legally enforceable. Although there are no express provisions in the handbooks which impose an obligation on banks to keep customer information secret, the general

[65] The report of this presentation is based on Professor Stanton's presentation at the Symposium.
[66] [1924] 1 KB 461 at 472-3.

principles in the handbooks are sufficient to support enforcement actions in the event of a major breach of the duty of bank secrecy. These principles require, amongst others, that a firm conduct business with integrity (Principle 1) and with due skill, care and diligence (Principle 2) and take reasonable care to organise and control its affairs responsibly and effectively (Principle 3).

5. Data protection law: The Data Protection Act 1998 applies to anyone who processes personal data, including banks. Schedule 1 of the Act establishes eight data protection principles, including that data shall be processed fairly and lawfully (Principle 1) and that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of or destruction of, or damage to, personal data (Principle 7). Principle 7 essentially provides for an obligation to keep customer information secret.

6. European law: As a member state of the European Union (EU), the UK is also influenced by various relevant EU laws, including, for example, EU's third Money Laundering Directive[67] and the European Convention on Human Rights.

However, various AML and anti-tax evasion laws have made incursions to the duty of bank secrecy. The main AML legislation in the UK is the Proceeds of Crimes Act 2002 and the Monetary Laundering Regulations of 2007, which establish a regime of "suspicion based" reporting of money laundering activities that directly overrides the duty of secrecy. The definition of suspicion is central to the regime. According to the Court of Appeal in *R v Da Silva*, a "vague feeling of unease would not suffice. But the statute does not require the suspicion to be 'clear' or 'firmly grounded and targeted on specific facts', or based upon 'reasonable grounds'."[68]

[67] Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
[68] [2007] 1 WLR 303.

Access to bank account information by the UK tax authorities is the second well-established statutory inroad into the duty of bank secrecy. Her Majesty's Revenue and Customs (HMRC) has extensive powers under Schedule 36 of the Finance Act 2008 to require the production of information or documents which are reasonably required for the purpose of checking a person's tax position. Moreover, UK is one of a number of European countries which have entered into agreements with the US concerning FATCA with the aim to support the US legislation, to reduce some of the administrative burdens placed on UK financial institutions and to ensure compliance with domestic data protection legislation.

It is worth noting that not all modern developments reduce the width of bank secrecy. The Data Protection Act 1998 and the developing law and practice relating to cybercrime all seek to maintain customer secrecy rather than breach it.

Bank secrecy issues form part of a larger picture of the development of professional standards in the financial services industry. Regulators have taken a proactive approach in ensuring that management imposes an acceptable culture on those working within firms. A failure to maintain bank secrecy tends to lead to a regulator responding that systems should have been in place to avoid it.

XI. Bank Secrecy in the United States[69]

Lissa Lamkin Broome, Wells Fargo Professor of Banking Law, University of North Carolina

The US has several statutes which impose duties on banks to keep customer information secret. [70] The most significant statute protecting financial privacy, the Right to Financial Privacy Act of 1978 (RFPA),[71] was enacted by Congress in response to a US Supreme

[69] The report of this presentation is based on Professor Broome's presentation at the Symposium.
[70] See, e.g., the Currency and Foreign Transactions Reporting Act of 1970 and the Right to Financial Privacy Act of 1978.
[71] 12 U.S.C. §§ 3401-3422.

Court case, *Untied States v. Miller*.[72] That case held that a customer did not have an expectation of privacy in account records maintained by a bank. The RFPA then imposed some limits on the power of the federal government to obtain customer financial records. Any financial records sought must be "reasonably described" and either (1) the customer authorised the disclosure, (2) there is an administrative subpoena, (3) there is a search warrant, (4) there is a judicial subpoena, or (5) there is a formal written request from a federal government authority.[73] If the government seeks information about a customer's account, the bank must notify that customer.

There are numerous exceptions to the RFPA that allow banks to disclose customer information. Several exceptions can be found in the RFPA itself: for example, a bank may (1) disclose information related to federal financial agency supervisory activities;[74] (2) notify a government authority about information related to a customer that may indicate a violation of a statute or regulation;[75] and (3) report financial records or information required to be reported by any federal statute.[76]

Two other federal statutes permit banks to share customer information in certain circumstances with nongovernment activities but set out very specific and limited purposes for this information sharing. The first statute is the Fair Credit Reporting Act (FCRA) of 1970, which requires fair and accurate reporting of customers' personal financial information by banks to a consumer reporting agency, such as Equifax and TransUnion.[77] The second statute is the Gramm-Leach-Bliley Act of 1999, which addressed the ability of financial institutions to share customer information with their affiliates and non-affiliates.[78] It permits sharing of customer information by financial institutions with their affiliates; sharing of information with non-affiliates is permitted

[72] 425 U.S. 435 (1976) (individuals have no Fourth Amendment expectation of privacy in their financial records while these records are in the hands of a third party like a bank).
[73] 12 U.S.C. § 3402.
[74] 12 U.S.C. § 3413(b).
[75] 12 U.S.C. § 3403(c).
[76] 12 U.S.C. 3413(d).
[77] 15 U.S.C. §§ 1681-1681x.
[78] 15 U.S.C. § 6801-6827.

only if the customer has been given the opportunity to "opt-out" such information sharing and has not opted out.

A number of AML and CFT laws create further inroads into the bank secrecy obligation. The Bank Secrecy Act (BAS) of 1970 contains two significant reporting requirements for financial institutions: currency transaction reports (CTRs) and suspicious activity reports (SARs).[79] A CTR must be filed for cash transactions exceeding a daily aggregate amount of US$ 10,000 by, through, or to the financial institution. A SAR relates to "any suspicious transaction relevant to a possible violation of law or regulation."[80] Suspicious transactions include criminal violations, potential money laundering and terrorism financing. Financial institutions are not allowed to notify their customers that a CTR or SAR has been filed.[81] After the terrorist attacks on 11 September 2011, the PATRIOT Act was enacted. [82] The statute adopted a "know your customer" standard for financial institutions in verifying the identity of new account holders.[83]

Other US statutes and programmes have significant impact on foreign banking operations outside the US. These include various sanctions programmes administered by the Office of Foreign Asset Control and the Treasury Department, as well as FATCA. The aim of FATCA is to ensure that foreign banks are not used to evade US tax. It requires foreign financial institutions to report information on their US account holders to either the foreign government (which in turn reports such information to the IRS) or directly to the IRS.[84] If foreign banks do not report this information as required by FATCA, the US financial institutions are required to impose a 30% withholding tax on

[79] Other reports include Reports of International Transportation of Currency or Monetary Instruments (CMIRs), and Reports of Foreign Bank and Financial Accounts (FBARS).
[80] 31 U.S.C. § 5318(g)(1).
[81] 31 U.S.C. § 5318(g)(2).
[82] The full name of the statute is Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. It included Title III, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (IMLAFAT).
[83] § 326, 31 U.S.C. §§ 53118(i)(1); 31 C.F.R. chapter X.
[84] Nathan Newman, New Individual Accounts under FATCA Intergovernmental Agreements, BNA Banking Rep. (25 November, 2014). As a result of FATCA, some US citizens have renounced their citizenship. Dylan Griffiths, Americans Give Up Passports As Asset-Disclosure Rules Start, BNA Banking Daily (8 August, 2014).

payments they make to those foreign banks. FATCA essentially deputised foreign banks as part of the US enforcement mechanism, in disregard of bank secrecy concerns in foreign countries.

Notably, in the post 9/11 world, concerns over bank secrecy take secondary importance as the US fights against money laundering, terrorist financing and tax evasion.

XII. Bank Secrecy in Hong Kong[85]

Stefan Gannon, Executive Director & General Counsel, Hong Kong Monetary Authority

In Hong Kong, a bank's duty to keep its customers' information confidential is based on common law and is well-established. The leading authority remains the UK decision in *Tournier*, in which the Court of Appeal held that the duty of confidentiality is an implied term of the contract between a banker and his customer. *Tournier* was applied in Hong Kong in the Hong Kong Court of Appeal decision in *F.D.C. Co Ltd and Others v The Chase Manhattan Bank, N.A.*("*F.D.C.*").[86]

The duty of confidentiality arises when a banker-customer relationship is established. The question of who is the "customer" is therefore relevant. While there is no statutory definition of "customer" in the Banking Ordinance (BO),[87] "customer" is defined in a number of bank merger ordinances[88] as any person having a banking account, a loan account or other dealing, transaction agreement or arrangement with the relevant merging bank. In the non-statutory code entitled "Code of Banking Practice",[89] "customer" and "personal customer" are used interchangeably to mean private individuals who (1) maintain an account in Hong Kong; or (2) act as guarantors or

[85] The report of this presentation is based on Mr. Gannon's presentation at the Symposium.
[86] [1990] 1 HKLR 277.
[87] Chapter 155 of the Laws of Hong Kong.
[88] See for example, the Bank of China (Hong Kong) Limited (Merger) Ordinance (Chapter 1167 of the Laws of Hong Kong).
[89] The Code was issued jointly by the Hong Kong Association of Banks and the Hong Kong Association of Restricted Licence Banks and Deposit-taking and endorsed by the Hong Kong Monetary Authority.

providers of third party security for a borrower.[90] The definition of "customer" has also been considered in a number of UK cases.[91] The case law, however, is not conclusive as to whether a person becomes a customer of a bank only in relation to services provided by the bank that constitute "banking business" as defined in the BO, or whether a person can become a customer of a bank in relation to any service provided by that bank that involves maintaining an account of any sort.

A bank's duty of confidentiality is supplemented by, amongst others, the Personal Data (Privacy Ordinance),[92] which protects the privacy of individuals in relation to their personal data, and the Code of Banking Practice, which provides that banks should treat their customers' and former customers' banking affairs as private and confidential.

As noted in *Tournier*, the banks' duty of confidentiality is subject to four exceptions:

1. Where disclosure is under compulsion by law: In Hong Kong, a bank may be compelled by a court order to disclose its customers' information in legal proceedings or by statutory provisions which either require or permit disclosure of confidential information by banks without consent from their customers. These provisions can be broadly divided into three categories: (a) prevention of crime;[93] (b) prevention of tax evasion;[94] and (3) regulation of the financial services industry.[95]

---

[90] See the definition of "Personal Customers" in the "Useful Definitions" section of the Code of Banking Practice.

[91] For example, in *The Great Western Railway Company v The London and County Banking Company Limited* [1901] AC 414, the House of Lords held that a customer of a bank was someone who had an account with the bank and the fact that the bank had for many years been accustomed to cash cheques made payable to a person did not make that person a customer.

[92] Chapter 486 of the Laws of Hong Kong.

[93] Some of the relevant provisions include:

- ss 25A of the Drug Trafficking (Recovery of Proceeds) Ordinance (Chapter 405 of the Laws of Hong Kong);
- ss 5 and 25A of the Organised and Serious Crimes Ordinance (Chapter 455 of the Laws of Hong Kong);
- ss 12 and 14 of the United Nations (Anti-Terrorism Measures) Ordinance (Chapter 575 of the Laws of Hong Kong);
- ss 67 of the Police Force Ordinance (Chapter 232 of the Laws of Hong Kong);
- ss 13 and 14 of the Prevention of Bribery Ordinance (Chapter 201 of the Laws of Hong Kong);

2. Where there is a duty to the public to disclose: The exception applies to situations where a public duty to disclose outweighs the private right to confidentiality. Commentators suggest that this qualification may be invoked to deal with situations arising in a cross-border context and to which the "compulsion by law" qualification does not necessarily apply (for example, major cases of corruption, terrorism and money laundering in connection with which a reputable bank might not wish to be seen to be withholding relevant information).[96]

3. Where the interests of the bank require disclosure: This qualification does not cover all disclosure which is to the bank's advantage. The disclosure must be limited strictly to information necessary to protect the bank's interest.[97] In *F.D.C.*, each plaintiff (each a customer of the Hong Kong branch of the defendant bank) applied for and obtained in Hong Kong an interim injunction against the bank to restrain it from disclosing bank records of that plaintiff to the IRS to comply with a US court order for production of those records. The bank applied to the High Court of Hong Kong to have those injunctions discharged and argued that it was in the bank's interest to disclose as it would otherwise be in contempt of the US court. This argument was rejected by the Hong Kong Court of Appeal on the ground that the bank's interest in disclosure was of a different character to that contemplated in *Tournier*. The court held that this qualification only applied in respect of the interests

---

- ss 9, 11 to 13 of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Chapter 615 of the Laws of Hong Kong); and
- s 5 of the Mutual Legal Assistance in Criminal Matters Ordinance (Chapter 525 of the Laws of Hong Kong).

[94] Some of the relevant provisions include:

- ss 4, 49, 51 and 51B of the Inland Revenue Ordinance (Chapter 112 of the Laws of Hong Kong); and
- ss 4 and 5 of the Inland Revenue (Disclosure of Information) Rules (Chapter 112BI of the Laws of Hong Kong).

[95] See, e.g., ss 55, 63, 117, 120 and 121 of the Banking Ordinance.

[96] Proctor, C., The Law and Practice of International Banking, Oxford University Press, 2010, at paragraphs 42.49-55.

[97] Neate, F. W. & Godfrey, G, Bank Confidentiality, 5th Edition, Bloomsbury Professional, 2011, at paragraph 11.7.

of ordinary banking practice which are narrow in nature, such as when it is "necessary to sue upon an overdraft or matters of that kind."[98]

4. Where the disclosure is made by consent of the customer: A customer's consent may be express or implied and it may be given to disclose the general state of the customer's account or only such information as is specified by the customer.

As part of its global fight against tax evasion, Hong Kong has recently entered into Tax Information Exchange Agreements with the US, Denmark, the Faroes, Greenland, Iceland, Norway and Sweden.[99] Hong Kong has also signed a "model II" intergovernmental agreement with the US to implement FATCA.[100] In addition, Hong Kong has enacted an Anti-Money Laundering Ordinance and issued a revised guideline on AML and CFT in 2012. Notably, the FATF recognised that Hong Kong had made significant progress in addressing the deficiencies identified in its 2008 mutual evaluation report.[101]

Despite increased gateways for the disclosure of banking information, there are sufficient in-built limitations under Hong Kong law to maintain an appropriate level of confidentiality in relation to the customer-banker relationship.

XIII. Bank Secrecy in Singapore[102]

Sandra Booysen, Assistant Professor, National University of Singapore

Bank secrecy in Singapore is governed by section 47 of the Banking Act.[103] Section 47(1) states that "[c]ustomer information shall not, in any way, be disclosed by a bank in

---

[98] *F.D.C.*, per Silke, JA at 292.
[99] See the Inland Revenue Department website, <www.ird.gov.hk/eng/tax/dta_tiea_agreement.htm>.
[100] See the press release "HK and US sign agreement to facilitate compliance with FATCA by financial institutions in HK (with photos)" on the Hong Kong Government website, <www.info.gov.hk/gia/general/201411/13/P201411130432.htm>.
[101] See "Follow-up report to the mutual evaluation report of Hong Kong, China" on the FATF website, <www.fatf-gafi.org/countries/d-i/hongkongchina/documents/followupreporttothemutualevaluationreportofhongkongchina.html>.
[102] The report of this presentation is based on Professor Booysen's presentation at the Symposium.
[103] Chapter 19 (2008 Revised Edition) of the Singapore statutes.

Singapore or any of its officers to any other person except as expressly provided in this Act."[104] Customer information includes information relating to a customer's accounts, deposits, investments and safe custody arrangements.[105] "Customer", however, is not defined in the Banking Act. The starting point would be the common law meaning, namely any person who has an account with a bank,[106] or for whom the bank has agreed to open an account.[107] Whether the concept of "customer" extends to less traditional, but today standard, banking relationships is less clear.

Prior to the wholesale reform of Singapore's bank secrecy regime in 2001, there was general consensus that the law on bank secrecy derives from both common law rules, which essentially followed *Tournier*, and banking legislation. After the reform in 2001, two opposing views emerged. One was that the common law rules and the statutory scheme continued to co-exist to the extent that they were compatible, failing which the statue prevailed.[108] The other view was that the statutory scheme completely replaced the common law rules.[109] The question was addressed in the Singapore Court of Appeal decision in *Susilawati v American Express Bank Ltd* ("*Susilawati*") in 2009. The court held that in light of the plain wording of section 47 of the Banking Act, the "current statutory regime on banking secrecy leaves no room for the four general common law exceptions expounded in *Tournier* to co-exist" and that the statutory regime is the "exclusive

---

[104] A "bank in Singapore" includes the Singapore branches and offices of a bank incorporated outside of Singapore; an officer of a bank in Singapore includes its directors, secretary and employees, and a "person" includes a corporation, see Banking Act, Chapter 19 (2008 Revised Edition), s 2. The Interpretation Act, Chapter 1 (2002 Revised Edition), s 2 says that a "person" includes a company, association or body of persons, whether corporate or unincorporate.

[105] Banking Act, Chapter 19 (2008 Revised Edition), s 40A. Information that does not identify a particular customer or group of customers is not caught, see *Teo Wai Cheong v Crédit Industriel et Commercial* [2011] SGCA 13 at [23] as follows: "In our view, s 47(1) of the Banking Act does not prohibit the disclosure of 'customer information' where the customer cannot be identified". The court considered that disclosure of telephone conversations with clients identified as Client A, B or C would be disclosure that is not referable to a named customer.

[106] *Great Western Railway Co v London & County Banking Co* [1901] AC 414; *Cmmrs of Taxation v English Scottish & Australian Bank Ltd* [1920] AC 683.

[107] *Woods v Martins Bank* [1959] 1 QB 55.

[108] Poh Chu Chai *Banking Law* (Lexis Nexis, Singapore, 2007), p 247 – 248; Poh Chu Chai *Law of Banker and Customer* (Fifth Edition, Lexis Nexis, Singapore, 2004) p 574 - 575.

[109] E P Ellinger "Disclosure of Customer Information to a Bank's Own Branches and to Affiliates" [2004/2005] 20 BFLR 137 at 137.

regime governing banking secrecy in Singapore".[110] The court's view has significant implications for the remedies available for breaches of the bank's secrecy obligation. The statutory regime provides that a breach of the duty of secrecy is punishable by fine and/or imprisonment and it makes no provision for damages to be paid to the customer. [111] If this is the exclusive regime governing bank secrecy, it seems to follow that a customer can no longer claim compensation for the loss suffered from a breach of the duty of secrecy.[112]

The bank's duty of secrecy under the Banking Act is not absolute. The Third Schedule to the Banking Act sets out a range of circumstances under which disclosure of customer information is permitted. For example, banks may disclose customer information with the customer's written permission.[113] Singapore banks invariably include some form of consent to disclosure in their standard terms and conditions (T&C). It is argued that broad T&C consent given at the time of opening the account does not generally satisfy the meaning of permitted disclosure as contemplated by the Third Schedule since such consent is generally given when the relevant customer does not have a specific disclosure in mind and therefore does not have an opportunity to discriminate between favourable and unfavourable disclosures. By contrast, the primary idea behind the written permission exception in the Third Schedule is to cover instances of disclosure which the customer desires in his own interests.

Apart from the Third Schedule, a number of initiatives operating outside the Banking Act make further inroads to the bank secrecy obligation. These inroads centre around the triumvirate of international tax cooperation, AML and CFT.

---

[110] [2009] 2 SLR(R) 737 at [67].
[111] Banking Act, Chapter 19 (2008 Revised Edition), s 47(6).
[112] Customers may seek compensation through other means, the most promising of which would be to bring an action based on breach of a duty of confidence.
[113] Banking Act, Chapter 19 (2008 Revised Edition), Third Schedule, Part I, para 1.

1. International tax cooperation: Singapore has embraced the OECD initiatives to combat tax evasion through a more extensive exchange of information regime[114] and has taken steps to facilitate compliance by Singapore financial institutions with the FATCA.[115]

2. AML legislation: Singapore's primary AML legislation comprises the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act ("CDSA")[116] and the Mutual Assistance in Criminal Matters Act (MACM).[117] Under CDSA, a public prosecutor may apply to the High Court for an order against a financial institution to disclose material for investigations into a long list of offences including drug dealing, terrorist financing and tax evasion.[118] Additionally, the CDSA imposes an obligations on financial institutions to report their knowledge or suspicion that a property has connection with criminal conduct.[119]

---

[114] For example: on 14 May 2013, Singapore's Ministry of Finance, the MAS and the Inland Revenue Authority of Singapore announced a strengthening of Singapore's international exchange of information framework to combat cross-border tax offences, <http://www.iras.gov.sg/irasHome/page03a.aspx?id=14926>; on 29 May 2013, the Ministry of Finance subsequently announced that Singapore had signed the Convention on Mutual Administrative Assistance in Tax Matters, which "will expand Singapore's network of EOI partners by 13 jurisdictions, including Brazil and the United States", <http://www.iras.gov.sg/irasHome/page03a.aspx?id=14994>.

[115] See, for example Yasmine Yahya "Eye on the Economy; Bitter pill to swallow to keep money clean", *Straits Times* 21 January 2014.

[116] Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A, 2000 Revised Edition) of the Singapore statutes ("CDTA").

[117] Mutual Assistance in Criminal Matters Act (Chapter 190A, 2001 Revised Edition) of the Singapore statutes.

[118] CDTA, s 31(5).

[119] CDTA, s 39(1). Criminal conduct is defined as a serious offence or a foreign serious offence. The Second Schedule sets out a list of serious offences. A foreign serious offence is basically one that offends the laws of another country and would be a serious offence if committed in Singapore. Foreign tax offences are also foreign serious offences. Drug dealing is treated separately, and defined in the First Schedule.

3. CTF legislation: Singapore's main CTF legislation is the Terrorism (Suppression of Financing) Act (TSFA),[120] which requires, amongst others, that persons with relevant information or in possession of terrorist property to notify the police.

To the extent that the CDSA, MACM and TSFA expand the situations in which banks are permitted to disclose customer information, it is a warranted and rational extension of the principles underlying the exceptions to bank secrecy obligations.

PART THREE. COMMENTS AND DISCUSSIONS

A few recurring themes emerged during the comment and discussion sessions.

First, certain reporting obligations imposed by regulators on financial institutions are arguably too extensive and onerous. The reporting requirements under the Dodd Frank Act[121] in respect of swap transactions serve as a good example. These requirements have broad extra-territorial effects. For instance, parties to swap transactions conducted in a non-US country (say India) between a US bank with an Indian bank on a swap denominated in Rupee may be required to report detailed information about these transactions to regulators in the US. Since the only element connecting the US with these transactions is that one party to these transactions is a US bank, the connection is arguably too weak to justify subjecting such transactions to the extensive reporting requirements under Dodd Frank. The requirements under Dodd-Frank might also apply to swap transactions between two non-US parties. For example, if a European bank deals with a non-US customer on a dollar swap and the bank calls its US branch to determine the pricing of the swap, the call to the US branch is arguably sufficient to

[120] Terrorism (Suppression of Financing) Act (Cap 325, 2003 Revised Edition). See also the second reading of the Terrorism (Suppression of Financing) Bill, Singapore Parliamentary Debates, vol 75, col 77 (22 February 2000, Mr. Wong Kan Seng).
[121] The Dodd–Frank Wall Street Reform and Consumer Protection Act (Pub.L. 111–203, H.R. 4173).

bring the transaction within the ambit of US law and hence the requirements under Dodd Frank. As a result, some market participants have moved away from using the US dollars as the currency of choice for their transactions to avoid US regulatory requirements.

Second, various jurisdictions have different and sometimes conflicting rules in respect of the bank's obligation to keep customer information secret and the related obligation to report customer information to domestic or foreign regulators under specified circumstances. Banks are sometimes forced to decide, at the risk of liability, whether to comply with the disclosure obligation in one jurisdiction or the duty to keep customer information confidential in another jurisdiction. This is clearly undesirable. Hence, there is a pressing need to identify and to resolve the conflicting requirements between different jurisdictions.

Third, the growing trend towards automatic exchange of information between entities in different jurisdictions might lead to problems. Automatic exchange of information not only poses considerable administrative burdens on the transmitting entity, but also tends to reduce the ability of the transmitting entity to control potential confidentiality risks posed by the receiving entity, e.g., its failure to comply with conditions attached to the relevant data transmission. An associated issue relates to the appropriate conditions that should be imposed on the receiving entity; arguably there should be proper restrictions on the purposes for which the receiving entity may use the relevant confidential information as well as requirements on that entity to prevent on-going disclosure of confidential information to other entities without prior permission.

Fourth, a distinction has to be drawn between a bank's disclosure of information to private entities (e.g., other banks), its home authorities, and foreign authorities. The level of protection offered by bank secrecy laws in the surveyed jurisdictions differs significantly in respect of disclosure of information to private entities. By contrast, all jurisdictions appear to provide extensive exemptions to enable banks to disclose customer information to their home authorities, in particular, financial regulators and

tax authorities. Disclosure of information to foreign authorities is more controversial. For example, participants from common law countries seemed to disagree whether such disclosure would fall within one of the qualifications to the bank secrecy obligation set out in the leading case of *Tournier*.

Fifth, vigorous enforcement of AML and CTF legislation has also caused banks to "de-risk", that is, decline to accept or serve customers from certain jurisdictions or background, thereby pushing these customers to smaller institutions. This creates additional risks since those smaller institutions tend to have less comprehensive compliance programmes and are more difficult to monitor or regulate.

Finally, participants discussed the circumstances under which a bank can rely on a consent clause in a banker-customer agreement to disclose customer information. The answer is not clear-cut and has to be decided on a case-by-case basis. Relevant considerations would include, for example, the scope of the consent clause, the nature of the relevant banker-customer relationship and whether the customer's attention was drawn to the consent clause.