Excerpt from Chetan Phull, *Big Data Law in Canada* (Toronto: Smartblock Law, 2019) at 47-55, 126-131. Reproduced for inclusion in seminar materials for the Blockchain Technology Symposium 2021, with the author's and publisher's respective consents.

CHAPTER 5:

DIGITAL AUTHENTICATION

I. The Present Law of Identity Authentication

Access to property and information in digital form, through online portals, must be safeguarded. Under PIPEDA, this duty arises from the "reasonable security arrangements" required to prevent unauthorized access. Proper user authentication practices are a crucial aspect of preventing such unauthorized access.

> [See PIPEDA, Sch. 1, Principle 4.7; OPC's TJX/Winners decision (PIPEDA Report of Findings #2007-389, Sep 25, 2017) at paras. 68-70.]

Authentication issues apply to any aspect of digital life where access is intended to be restricted to one or more specific individuals. Such issues most obviously arise in the financial industry, in the form of:

- fraudulent payment instructions given by e-mail or phone;
- interception of money transfer by e-mail hack; and

- fraudulent 2-factor authentication facilitated by SIM-swapping.

[Compare *Du v. Jameson Bank*, 2017 ONSC 2422 at paras. 64 and 78 with the *Lanark Leeds* case, 2019 CanLII 69697 (ON SCSM) at paras. 56-65 re payment instructions by e-mail and e-mail hacks; OPC, "A full year of mandatory data breach reporting: What we've learned and what businesses need to know" (Oct 31, 2019) re fraud through impersonation over the phone; *Michael Terpin v. AT and T Inc et al*, No. 2:2018cv06975, Doc 29 (C.D. Cal. 2019) re $24 million crypto theft through SIM-swap attack; Sean Coonce, "The Most Expensive Lesson Of My Life: Details of SIM port hack" (Medium, May 20,2019). See also cases on insurance coverage due to fraudulent payment instructions, cited in subsection II of Chapter 3 under the paragraph beginning with "Insurance coverage may also become an issue….".]

Apart from the general duty in PIPEDA to safeguard against unauthorized access, the only law covering digital authentication in a specific and targeted manner is the *Directive on Identity Management* ("**ID Directive**"), and *Standard on Identity and Credential Assurance* ("**ID Standard**"). The former was last amended in 2019, while the latter was last amended in 2013. Both documents derive their authority from the *Financial Administration Act*. Pursuant to these documents, the importance of accurate authentication must be assessed according to four levels. Depending on the applicable level, a different set of requirements apply.

[See Government of Canada, *Directive on Identity Management* (updated Jul 1, 2019), incl. ss.2 and A.2.3 of same; Government of Canada, *Standard on Identity and Credential Assurance* (updated Feb 1, 2013); Government of Canada, *Policy on Government Security* (updated Jul 1, 2019), s.2; *Financial Administration Act*, RSC 1985, c F-11, s.7.]

However, the determination of which level applies, and whether requirements for the applicable level are met, appear to involve much discretion. The ID Directive and ID Standard also do not address specific authentication issues arising specifically in the online context, for example: with respect to encryption standards for online authentication operations, integrity of personalised security credentials, etc. Moreover, the ID Directive and ID Standard are limited to the public sector, and their initial threshold for applicability cannot easily be ported to the private sector.

The most useful guidance on digital authentication in the private sector is the OPC's *Guidelines for identification and authentication* ("**OPC ID Guidelines**"). The OPC ID Guidelines are not law *per se*, but helpfully tie digital authentication

best practices to the core privacy principles arising from PIPEDA. The OPC ID Guidelines focus on the following topics in particular:

- multi-factor authentication;
- scope of data collection;
- data retention periods;
- consent to collect and process information;
- employee training;
- audit records;
- cybersecurity controls to avoid "man in the middle" attacks;
- data protection;
- trusted ID documents;
- trusted third parties when ID management is outsourced;
- careful approach to biometrics authentication.

[See OPC, "Guidelines for identification and authentication" (June 2016).]

A more helpful and detailed authentication guide has been provided by the Communications Security Establishment ("**CSE**"), in the *User Authentication Guidance for Information Technology Systems* ("**CSE Guidance**"). This document applies to federal government institutions only, but should be treated as a standard within the public provincial and private sectors as well. The CSE Guidance provide specific authentication guidance to combat specific threats. The document borrows "four levels of increasing authentication assurance" from the U.S. NIST framework (referenced below), and stresses the importance of multi-factor authentication in the context of a token authenticator. It also discusses token threats and mitigations, salting and hashing protocols, authentication monitoring, and user education. The high level of rigour can be explained in part by the general mandate of the CSE, which is discussed further in Chapter 9.

[Communications Security Establishment, *User Authentication Guidance for Information Technology Systems* (Apr 4, 2018), ss.2.1, 4.]

The Treasury Board has also provided technical authentication specifications for participation in the "Canada cyber-authentication environment." These specifications appear in the *Cyber-Authentication Technology Solutions Interface Architecture and Specification Version 2.0 (CATS2 IA&S)*, and appear to be regularly updated. They should be closely considered by the development team responsible for the authentication gateway.

> [Treasury Board, Deployment Profile for CATS2 IA&S (last modified Feb 20, 2018); Government of Canada, *Guideline on Defining Authentication Requirements* (Nov 30, 2012).]

In addition to the above measures, efforts are being made in Canada to codify a more robust, broader framework for digital authentication. The Canadian federal and provincial governments, along with other private sector participants, are working with the Digital ID & Authentication Council of Canada ("**DIACC**") to manage and deliver digital ID services across government and commercial platforms.

> [See Government of Canada, "Canada's trusted digital identity vision" (video, Oct 11, 2018); Government of Ontario, "Ontario Digital Service: key priorities" under "Implement a common approach to digital identity" (last updated Aug 9, 2019); DIACC, "About Us" (2019).]

The DIACC is presently developing a domestic industry framework, called the Pan-Canadian Trust Framework (the "**PCTF**"). At the time of publication, most material PCTF documents are still in draft. The PCTF is anticipated to provide common terms, expectations, and defined processes to assist with contract drafting for digital ID matters. However, there are no prescribed or model contracts anticipated for the **PCTF**.

> [See DIACC, "Pan-Canadian Trust Framework Work Program"; DIACC, "Pan-Canadian Trust Framework Overview" (Aug 2016) at 8.]

It is probable—or at least hoped—that **PCTF** drafting efforts include consideration of foreign "open banking" laws. Open banking refers to the porting and transfer of customer banking data, inclusive of transactional information, for customers to more easily compare financial services and switch providers. So far, this new business model has been mandated by legislation in Europe, U.K.,

and Australia, each on grounds of privacy and big data competition (the latter of which is discussed in Chapter 11).

[See European Directive 2015/2366 re PSD2 (landing page); CME, "The Retail Banking Market Investigation Order 2017" (UK, Feb 2, 2017); CMA, "Explanatory Note: The Retail Banking Market Investigation Order 2017" (UK, Feb 28, 2017); *Treasury Laws Amendment (Consumer Data Right) Act 2019*, No. 63, 2019 (Australia).]

Further to its open banking mandate, the E.U. Parliament and Council passed the eIDAS Regulation in 2014. This regulation "establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication."

[See eIDAS Regulation, Art. 1(c); European Commission, "eIDAS for SMEs" (last updated Nov 29, 2018).]

The following year, the E.U. Parliament and Council passed the PSD2 Directive ("**PSD2**"). The PSD2 stipulates that "strong customer authentication" requirements must be legislated by all Member States. The term "strong customer authentication" ("**SCA**") is defined as a standard for multi-factor authentication. The PSD2 also requires development of "common and secure … communication" ("**CSC**"), for various purposes including identification and authentication.

[See European Directive 2015/2366 re PSD2, Arts. 4(30), 97, 98(1)(d).]

In 2017, the U.K.'s Competition & Markets Authority ("**CMA**") supported open banking by means of an order against the U.K.'s largest banks. That order required the development of banking standards covering various topics, including an open application program interface ("**API**"), data formats, and security. Authorization and authentication standards were part of the mandate for security standards. In the order, the definitions for SCA and CSC were deferred to the European definitions, to be provided by the European Banking Authority ("**EBA**").

[See CME, "The Retail Banking Market Investigation Order 2017" (UK, Feb 2, 2017); CMA, "Explanatory Note: The Retail Banking Market Investigation Order 2017" (UK, Feb 28, 2017).]

In 2018, the two European standards—SCA and CSC—were clarified by the EBA. As required under the PSD2, the EBA also issued Regulatory Technical

Standards ("**RTS**") for SCA and CSC. The RTS discusses multi-factor authentication in detail. Efforts to develop authentication standards under the open banking mandate continue in full force within Europe and the U.K.

> [See EBA press release re SCA and CSC (June 13, 2018); FCA, "FCA statement on EBA's draft PSD2 Guidelines and Opinion for banks and others involved in open banking" (UK, June 22, 2018); CMA, "Notice of approval of changes to the Agreed Timetable and Project Plan" (UK, July 26, 2018); EBA's opinion re elements of CSC under PSD2 (June 21, 2019).]

In the U.S. context, President Obama proposed an Identity Ecosystem Framework ("**IEF**") in 2011. The IEF proposed the establishment of standards based on defined risk models. It further proposed to: "establish the accountability and remediation process when an identity credential is fraudulently issued or used or when other breakdowns in the Identity Ecosystem occur." However, other than for e-signatures, no federal U.S. law appears to have been legislated for authenticated login mechanisms for online portals.

> [See President Barak Obama, "National Strategy For Trusted Identities In Cyberspace" (April 2011, US); *Electronic Signatures in Global and National Commerce Act*, 15 U.SC. 96, §§ 7001-7006 ("ESIGN").]

U.S. rules for digital authentication were subsequently issued in the form of guidelines applicable to the federal public sector. These rules, called the NIST "Digital Identity Guidelines" ("**NIST Guidelines**"), were issued and updated in 2017. In concert with the standards mentioned above, the NIST Guidelines also discuss multi-factor authentication principles. With its three companion volumes, it comprehensively also covers technical authentication standards for enrollment and identity proofing requirements, authentication and lifecycle management, and federation and assertions.

> [See NIST, "Digital Identity Guidelines", SP 800-63-3, SP 800-63A, SP 800-63B, SP 800-63C (Dec 1, 2017).]

At the level of international law beyond the E.U., development of global digital ID standards is underway but still in its infancy. The most headway to date has been made by the Financial Action Task Force ("**FATF**"), an inter-governmental body tasked with setting international anti-money laundering standards. The FATF released draft guidance on digital ID ("**FATF Draft Guidance**") in mid-2019,

and a consultation period on the Draft Guidance ended in November 2019. Further amendments to the Draft Guidance are expected in February 2020.

[See FATF, "Public consultation on FATF draft guidance on digital identity" (Nov 2019), incl. "Appendix E: Overview of US and EU digital ID assurance frameworks and technical standards" at 70-73.]

As the foregoing discussion indicates, there are many sources of actual and persuasive law relating to digital authentication. It is an area in rapid and ongoing development. Until Canada's PCTF is finalized by DIACC, or a sector-agnostic standard for digital ID is legislated, legal counsel should consider digital ID standards with respect to all the authorities mentioned above.

II. Future Considerations Affecting Authentication Law

With regard to Canada's position on open banking, an Advisory Committee on Open Banking was launched in September 2018, and a Senate committee's report on open banking was issued as of June 2019. So far, however, the only significant mention of Canada's digital authentication requirements for open banking, are in that Senate committee's report. In that report, a bank simply expressed the need for "better authentication, password and security controls."

[See Department of Finance, "Minister Morneau Launches Advisory Committee on Open Banking" (Sep 26, 2018); BANC Committee Report, "Open Banking: What It Means For You" (June 2019) at 6, 26.]

With regard to ongoing development of the PCTF, the DIACC and CBA have each proposed looking to Estonia and India, as examples for how to implement digital ID legislative and policy frameworks. Canada subsequently entered into a Memorandum of Understanding with Estonia as of May 2018, "to define a common agenda and encourage closer ties … in the fields of digital government, the digital economy and related policy issues." It is understood that digital authentication falls into this mandate.

[See DIACC, "The Economic Impact of Digital Identity in Canada" (2018); CBA, "Canada's Digital ID Future - A Federated

> Approach" (Spring 2018); Memorandum of Understanding between Canada and Estonia re Digital Government and Economy (May 28, 2018).]

Moreover, legal developments are likely to shift with new technological means for authentication. Consider, for example, the recommendation by the Canadian Bankers Association ("**CBA**") for a blockchain-type solution to digital identity, which was independently also acknowledged by FATF. The CBA proposed:

> [A] federated identity system leverages multiple systems, eliminating reliance on a single service provider. In other words, there is no single point of control or failure that can compromise the entire system. … The decentralized network also reduces the risk of fraud by eliminating any "honeypots" of data that can be compromised.

> [See CBA, "Canada's Digital ID Future - A Federated Approach" (Spring 2018); FATF, "Public consultation on FATF draft guidance on digital identity" (Nov 2019) at 8, 12 re the use of distributed ledger technology for digital authentication; Daniel Therrien's "Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on Privacy of Digital Government Services" re Estonia's blockchain model (Jan 31, 2019).]

A blockchain solution for digital identity would involve more robust legal controls specific to the blockchain context. As noted in subsection III of Chapter 2, such controls should consider nodes as third-party data processors, data storage protocols, ledger integrity controls, etc.

In addition, as of June 2018, fintech legislative reform has permitted various types of financial entities to "provide identification, authentication or verification services." As the Canadian digital authentication legal framework matures, it should be expected that digital ID verification will become a commonly outsourced service to Canadian financial institutions, and foreign affiliates. It is plausible that the government may also run a registry of accredited third-party authentication vendors, further to a Senate committee's recommendation.

> [See *Trust and Loan Companies Act*, s.410(1)(h); *Bank Act*, ss.410(1)(h) and 539(1)(g); *Insurance Companies Act*, s.441(1)(i); and *Budget Implementation Act, 2018, No. 1*, S.C. 2018, c. 12; "17. Reliance on Third Parties" and "Interpretive Notice to Recommendation 17" in *FATF Recommendations* [Updated June 2019] at 16, 78; FATF's "Public consultation on FATF draft guidance on digital identity" at 20-22; BANC Committee Report, "Open Banking: What It Means For You" (June 2019) at 6.]

One subsector where outsourcing of digital ID services will increase, is digital asset services. This industry was recently legitimized under domestic virtual currency legislation, which was mandated internationally by FATF and is scheduled to come into force in June 2020. Moreover, in recent years, the crypto space has been deeply troubled by a lack of digital authentication guideposts. This has resulted in inadequate KYC during account setup, fraudulent online access to user accounts, and poor verification of investment instructions. Hence, in the crypto space, user authentication has presented exposure that service providers will now, most certainly, attempt to offload by hiring third-party authentication agents.

[See *Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2018*, "Description" within the "Regulatory Impact Analysis Statement"; FINA Committee Report, "Confronting Money Laundering and Terrorist Financing: Moving Canada Forward" (Nov 2018) at 64, Recommendation 26; CSA/IIROC Consultation Paper 21-402 (Mar 14, 2019) at 12 (5.2.4 "Systems and business continuity planning"), and at 25 ("Appendix C" under "7. KYC and suitability"); *Michael Terpin v. AT and T Inc et al*, No. 2:2018cv06975, Doc 29 (C.D. Cal. 2019) re $24 million crypto theft through SIM-swap attack; Sean Coonce, "The Most Expensive Lesson Of My Life: Details of SIM port hack" (Medium, May 20,2019).]

III. Conclusion

The digital economy is becoming increasingly important to daily life. Participation in the digital economy necessarily involves secure access to online portals. While the legal framework for digital authentication presently has patchwork application, the framework is undeniably on a fast course of development. Legal counsel in the Canadian digital ID industry should consider current laws in the public sector, unofficial laws in the private sector, draft documents for the developing Canadian framework, as well as foreign laws and guidance on digital ID. These materials will certainly feed into more broadly applicable legal authority, and should be considered by counsel now for early risk mitigation.

157. Office of the Privacy Commissioner of Canada, *Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy*, (Ottawa: OPC, 2019) at 13, 19, 53.

158. Office of the Privacy Commissioner of Canada, *Reforming Canada's privacy laws: Shifting from the whether to the how*, (Ottawa: OPC, 2019).

159. Office of the Privacy Commissioner of Canada, *Ten tips for addressing employee snooping*, (Ottawa: OPC, 2016).

160. Office of the Privacy Commissioner of Canada, *What you need to know about mandatory reporting of breaches of security safeguards*, (Ottawa: OPC, 2018).

161. Office of the Superintendent of Financial Institutions, *Federally Regulated Financial Institutions*, (Ottawa: OSFI, 2014) online <http://www.osfi-bsif.gc.ca/eng/wt-ow/pages/wwr-er.aspx>.

CHAPTER 5: DIGITAL AUTHENTICATION

Legislation, Regulations & Directives

162. *Bank Act*, SC 1991, c 46, ss 410(1)(h), 539(1)(g).

163. *Budget Implementation Act, 2018, No. 1*, SC 2018, c 12.

164. *Canada Gazette, Part I, Volume 152, Number 23: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2018*, (Ottawa: Department of Finance, 2018).

165. Competition and Markets Authority, *The Retail Banking Market Investigation Order 2017*, (UK: CMA, 2 February 2017).

166. *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC*, ["PSD2 Directive"] Arts 4(30), 97, 98(1)(d).

167. *Financial Administration Act*, RSC 1985, c F-11, s 7.

168. Government of Canada, *Directive on Identity Management*, (Ottawa: Treasury Board, 2019) ss 2, A.2.3.

169. Government of Canada, *Guideline on Defining Authentication Requirements*, (Ottawa: Treasury Board, 2012).

170. Government of Canada, *Policy on Government Security*, (Ottawa: Treasury Board, 2019) s 2.

171. Government of Canada, *Standard on Identity and Credential Assurance*, (Ottawa: Treasury Board, 2013).

172. *Insurance Companies Act*, SC 1991, c 47, s 441(1)(i).

173. *Memorandum of Understanding Between the Treasury Board of Canada Secretariat and the Ministry of Economic Affairs and Communications of the Republic of Estonia on Cooperation in the Field of Digital Government and Economy*, (Ottawa: Treasury Board of Canada Secretariat, 2018).

174. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Sch 1, Principle 4.7.

175. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, ["eIDAS Regulation"], Art 1(c).

176. Treasury Board Secretariat of Canada, *Cyber-Authentication Technology Solutions Interface Architecture and Specification Version 2.0 (CATS2 IA&S): Deployment Profile*, (Ottawa: Treasury Board, 2018).

177. *Treasury Laws Amendment (Consumer Data Right) Act 2019*, Act No 63 of 2019 (Australia) ["Consumer Data Right"].

178. *Trust and Loan Companies Act*, SC 1991, c 45, s 410(1)(h).

Jurisprudence

179. *Apache Corp. v. GAIC*, 662 Fed. Appx. 252 (5th Cir. Oct. 18, 2016).

180. *Brick Warehouse LP v Chubb Insurance Company of Canada*, 2017 ABQB 413 at paras 19-25 (CanLII).

181. *Dentons Canada LLP v. TGIC*, 2018 ONSC 7311 at para. 39 onward.

182. *Du v Jameson Bank*, 2017 ONSC 2422 at paras 64, 78 (CanLII).

183. *Electronic Signatures in Global and National Commerce Act*, 15 U.SC. 96, §§ 7001-7006 ("ESIGN") (LII).

184. *Medidata Solutions Inc. v. FIA*, 729 Fed.Appx. 117 (2d Cir. 2018).

185. *Michael Terpin v AT and T Inc et al*, 2018 No. 2:2018cv06975 - Document 29 (C.D. Cal. 2019).

186. Office of the Privacy Commissioner of Canada, *Report of an Investigation into the Security, Collection and Retention of Personal Information TJX Companies Inc./Winners Merchant International L.P.*, (Ottawa: OPC, 2007) paras 68-70.

187. *St. Lawrence Testing & Inspection Co. Ltd. v Lanark Leeds Distribution Ltd.*, 2019 CanLII 69697 (ON SCSM) at paras 56-65.

Regulatory Guidance & Other Secondary Sources

188. Canadian Bankers Association, *Canada's Digital ID Future - A Federated Approach*, White Paper (CBA, 2018).

189. Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada, "Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms", (2019) at 12, 25.

190. Communications Security Establishment, *User Authentication Guidance for Information Technology Systems* (Ottawa: CSE, Apr 2018).

191. Competition and Markets Authority, *Explanatory Note: The Retail Banking Market Investigation Order 2017,* (UK: Competition and Markets Authority, 28 February 2017).

192. Competition and Markets Authority, *The Retail Banking Market Investigation: Notice of approval of changes to the Agreed Timetable and Project Plan*, (UK: Competition and Markets Authority, 26 July 2018).

193. Department of Finance Canada, *Minister Morneau Launches Advisory Committee on Open Banking*, Press Release (Ottawa: Office of the Minister of Finance, 26 September 2018).

194. DIACC Member Consult Hyperion, *The Economic Impact of Digital Identity in Canada*, (Digital ID and Authentication Council of Canada, 2018).

195. DIACC Trust Framework Expert Committee, *Pan-Canadian Trust Framework Overview*, (Digital ID and Authentication Council of Canada, 2016) at 8.

196. Digital ID and Authentication Council of Canada, "Pan-Canadian Trust Framework Work Program" (12 February 2019), online: DIACC <https://diacc.ca/pan-canadian-trust-framework/>.

197. European Banking Authority, *EBA provides clarity to market participants for the implementation of the technical standards on strong customer authentication and common and secure communication under the PSD2*, Press Release (Paris: EBA, 13 June 2018).

198. European Banking Authority, *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, Opinion (Paris: EBA, 21 June 2019).

199. European Union, *eIDAS for SME - Electronic Identification, Authentication and Trust Services, Policy* (Brussels: EC, 29 November, 2018).

200. European Union, *Law Details: Information about Directive (EU) 2015/2366 on payment services including date of entry into force and a link to the summary*, (Brussels: European Commission, 2015).

201. Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, (Paris: FATF, 2019) at 16, 78.

202. Financial Action Task Force, *Public consultation on FATF draft guidance on digital identity*, (Paris: FATF, 30 November 2019) at 8, 12, 20, 22, 70-73.

203. Financial Conduct Authority, *FCA statement on EBA's draft PSD2 Guidelines and Opinion for banks and others involved in open banking*, Statements (UK: FCA, 22 June 2018).

204. Government of Canada, *Competition Bureau sues to shut down business directory scam*, (Ottawa: Competition Bureau, 2011).

205. Office of the Privacy Commissioner of Canada, *A full year of mandatory data breach reporting: What we've learned and what businesses need to know*, (Ottawa: OPC, 2019).

206. Office of the Privacy Commissioner of Canada, *Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on Privacy of Digital Government Services*, (Ottawa: OPC, 2019).

207. Office of the Privacy Commissioner of Canada, *Guidelines for Identification and authentication*, (Ottawa: OPC, 2016).

208. Ontario, *Ontario Digital Service: key priorities*, (Toronto: Government of Ontario, 2017).

209. Parliament, House of Commons Standing Committee on Finance, *Confronting Money Laundering and Terrorist Financing: Moving Canada Forward*, 42nd Parl, 1st Sess, (November 2018) (Chair: The Honourable Wayne Easter) at 64.

210. Paul Grassi et. al., *Digital Identity Guidelines*, SP 800-63-3, SP 800-63A, SP 800-63B, SP 800-63C (U.S. Department of Commerce: NIST, December 2017).

211. Sean Coonce, "The Most Expensive Lesson Of My Life: Details of SIM port hack" (20 May 2019), online: Medium <https://medium.com/coinmonks/the-most-expensive-lesson-of-my-life-details-of-sim-port-hack-35de11517124>.

212. Standing Senate Committee on Banking, Trade and Commerce, *Open Banking: What it means for you*, 42nd Parl, (June 2019) at 6, 26 (Chair: The Honourable Senator Doug Black, Q.C.).

213. Treasury Board of Canada Secretariat, *Canada's Trusted Digital Identity Vision*, (Ottawa: Treasury Board of Canada Secretariat, 2018).

214. United States of America, The White House, *National Strategy for Trusted Identities in Cyberspace – Enhancing Online Choice, Efficiency, Security, and Privacy*, White House Release (Washington: President Barack Obama, April 2011).

CHAPTER 6: CANADIAN ANTI-SPAM LEGISLATION ("CASL")

Legislation, Regulations & Directives

215. *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23, ["Canada's Anti-Spam Legislation" or "CASL"] ss 1(1), 3, 6-13, 15, 17, 19, 20(4), 24(2), 31-33, 39(b), 42-46, 52-54, 57-59.

216. *Electronic Commerce Protection Regulations*, SOR/2013-221, ss 3, 6.

217. Government of Canada, Order in Council 2013-1323, (3 December 2013).

218. Government of Canada, Order in Council 2017-0580, (2 June 2017).