Utah - Data Protection in the Financial Sector

TABLE OF CONTENTS

August 2020

1. INTRODUCTION

In Utah, collection and disclosure of personal information in the financial sector, including financial information, is governed by a few key privacy and insurance regulations. The Protection of Personal Information Act, §13-44-101 et seq. of the Utah Code ('PPIA') requires any person who conducts business in the state to maintain certain policies respecting the protection of personal information. However, many of these regulations provide exceptions for financial institutions. The Utah Administrative Code, Rule R590-206, details how licensed insurers in Utah must treat the non-public personal financial information of consumers. Additionally, the Financial Information Privacy Act, Utah Code § 7-1-1001 *et seq.* ('FIPA') and the Electronic Information or Data Privacy Act, Utah Code § 77-23c-102 *et seq.* ('EIDPA') limit and restrict both government's requests for personal information of customers from businesses and law enforcement's access to electronic records stored by businesses.

1.1. Legislation

- The PPIA requires businesses that maintain personal information to establish procedures to prevent the 'unlawful use or disclosure of personal information' and to destroy 'records containing personal information' not to be kept by the business (Utah Code § 13-44-201(2)). However, these rules do not apply to businesses that engage in financial activities (Utah Code Ann. § 13-44-103; § 6809(3) of Title 15 of the United States Code ('USC')); see also 12 USC § 1843(k)(4) (list of activities considered financial in nature).
- Insurance businesses that are required to obtain a license from the Utah Insurance Department (the 'Insurance Department') are subject to the privacy rules promulgated

by the Utah Insurance Commissioner (Utah Code § 31A-1-104; Utah Administrative Code Rule R590-206-1). These rules establish a framework for the treatment of non-public financial information gathered by licensed insurers.

- The FIPA blocks government entities from requesting an individual's personal financial information from a state or federally chartered financial institution without first obtaining written permission from the account holder or obtaining a court order (Utah Code Ann. § 7-1-1001(2).bb).
- The EIDPA establishes that a warrant is required when law enforcement seeks to access any data, including financial data, on electronic devices, and creates a 14-day notice requirement before the data that is subject to the warrant may be obtained (Utah Code § 77-23c-101.1 *et seq*.).

1.2. Supervisory authorities

The PPIA is enforced by the Utah Attorney General ('AG') (Utah Code §13-44-301). The AG is expressly authorised to protect Utah businesses and consumers from fraud, scams, and misuse of financial information. In particular, Utah Code §13-44-301 empowers the AG to enforce the PPIA, levy fines or other actions against violators as necessary, and inspect or review the records of suspected violators, among other actions.

Regulations promulgated by the Insurance Department are enforced by the Utah Insurance Commissioner (Utah Code § 31A-1-104; Utah Admin. Code R590-2016-1). The Insurance Department is empowered to enforce Utah Code's insurance-licensing provisions, adopt administrative rules for the governance of licensed insurers, implement those rules, and pursue breaches of the Utah Code or administrative rules.

2. PERSONAL AND FINANCIAL DATA MANAGEMENT

2.1. Legal basis for processing

The PPIA requires any person or entity (with the exception of financial institutions) that conducts business in Utah and maintains personal information to implement safeguards for preventing the unlawful use or disclosure of personal information. Further, such person or entity must destroy

records containing personal information 'that are not to be retained' by the collecting person or entity (Utah Code §13-44-201). The PPIA does not outline or require procedures for the collection, processing, or transfer of personal information beyond this.

The Utah Admin. Code R590-206-1 (the 'Code') governs the treatment of non-public financial data and non-public personal health information collected by licensed insurers (i.e., "licensees") in Utah. Under the Code, licensees are required to provide a clear and conspicuous notice that accurately reflects privacy policies and practices to customers and consumers, and it details the conditions under which a licensee may disclose non-public personal financial information (Section 12 of the Code). However, licensees who only disclose the non-public financial information to non-affiliated third parties, other than the ones authorised in Section 16 and 17 of the Code, do not need to provide the consumer with an initial notice (Section 5(1) of the Code). The notice must be delivered upon the initiation of the customer relationship, which is established when the licensee and the consumer enter a continuing relationship (Sections 4 and 5(1)of the Code).

Moreover, licensees are subject to not only initial privacy notice disclosures, but annual privacy notice updates (Section 7 of the Code). Please refer to Section 3 below for the required contents of the privacy notice.

2.2. Privacy notices and policies

Under the Code licensed insurers—licensees—in Utah must generally provide an initial, annual, and any later-revised privacy notice to consumers and notices must include (Section 7 of the Code):

- the categories of non-public personal financial information that the licensee collects;
- the categories of non-public personal financial information that the licensee discloses;
- the categories of affiliates and non-affiliated third parties to whom the licensee discloses non-public personal financial information, other than those parties to whom the licensee discloses information under Sections 16 and 17;
- the categories of non-public personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and non-affiliated third parties to whom the licensee discloses non-public personal financial information about the licensee's former customers, other than those parties to whom the licensee discloses information under Sections 16 and 17;
- if a licensee discloses non-public personal financial information to a non-affiliated third party under Section 14, and no other exception in Sections 16 and 17 applies to that disclosure, a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;

- an explanation of the consumer's right under Section 12(1) of the Code to opt-out of the disclosure of non-public personal financial information to non-affiliated third parties, including the methods by which the consumer may exercise that right at that time;
- any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act of 1970 (15 USC 1681a(d)(2)(A)(iii));
- the licensee's policies and practices with respect to protecting the confidentiality and security of non-public personal information; and
- any disclosure that the licensee makes under Subsection 7(2) of the Code.

Where a licensee is required to provide an opt-out notice they must provide clear and conspicuous notice to each of its consumers that accurately explains the right to opt-out and (Section (8) of the Code):

- that the licensee discloses or reserves the right to disclose non-public personal financial information about its consumer to a non-affiliated third party;
- that the consumer has the right to opt-out of that disclosure; and
- a reasonable means by which the consumer may exercise the opt-out right.

2.3. Data security and risk management

The PPIA requires any entity (with the exception of financial institutions) who owns or licenses computerised data that includes personal information concerning a Utah resident to notify the Utah resident if an investigation reveals any misuse of personal information that could be used for identity theft or fraud, whether such activity has actually occurred or is simply likely to occur (Utah Code § 13-44-202(1)(b)). However, notification is not required if, after a good-faith and reasonable investigation, the entity determines that it is unlikely the personal information has or will be used for fraud or identity theft. Notification must be provided in the most expedient time possible without unreasonable delay through first class mail, by telephone, or electronically (Utah Code § 13-44-202(2); Utah Code § 13-44-202 (5)).

The PPIA does not apply to a financial institution or affiliate of a financial institution, as defined in 15 USC § 6809 (Utah Code § 13-44-103). Generally, financial institution means any institution whose business involves financial activities or activities that are complementary to a financial activity, such as lending, insuring, financial advising, selling interest, underwriting, or as described in 12 USC 1843(k)(4) (15 USC §6809). A financial institution does not include:

- any person or entity subject to the Commodity Futures Trading Commission (15 USC §6809(3)(B)) or the Federal Agricultural Mortgage Corporation (15 USC §6809(3)(C)); or
- institutions chartered by the US Congress specifically to engage in transactions as described in 15 USC §6802(e)(1)(C) as long as such institutions do not sell or transfer non-public personal information to a non-affiliated third party (15 USC §6809(3)(D)).

2.4. Data retention/record keeping

Not applicable.

3. FINANCIAL REPORTING AND MONEY LAUNDERING

Under the Money Laundering and Currency Transaction Reporting Act, persons engaged in trade or business, other than financial institutions, are generally required to report the receipt of more than $10,000 through either 'one transaction' or 'two or more related transactions during one business day' to the State Bureau of Investigation (Utah Code § 76-10-1906(1)). Failure to comply with these reporting requirements can result in a misdemeanour or felony.

4. BANKING SECRECY AND CONFIDENTIALITY

Not applicable.

5. INSURANCE

Businesses that are required to obtain a license from the Utah Insurance Department are subject to the privacy rules promulgated by the Insurance Commissioner (Utah Code § 31A-1-104; Utah Admin. Code R590-206-1), as detailed in Sections 2 and 3 above. These rules require insurance companies to provide an initial notice of their privacy policies to new customers and a yearly update on their privacy policies to continuing customers. (R590-206-5(1)). Additionally, insurance companies must provide their customers with an opt-out notice and give them an adequate opportunity to

opt-out before disclosing their personal financial information to a third party (R590-206-8, 12). Failure to comply with these rules may result in 'forfeiture, penalties, and revocation of license' (R590-206-25).

There is a specific exemption for financial institutions that 'engage in activities [...] that do not require a license from the Utah insurance commissioner' (Utah Admin. Code R590-206-2(4)).

6. PAYMENT SERVICES

Not applicable.

7. DATA TRANSFERS AND OUTSOURCING

Not applicable.

8. BREACH NOTIFICATION

Please see section 2.3.

9. FINTECH

Not applicable.

10. ENFORCEMENT

The PPIA is enforced by the Utah AG (Utah Code §13-44-301). A person who violates the PPIA is subject to fines ranging from $2,500-$100,000 for the volume of consumers the violations impact.

Regulations promulgated by the Insurance Department are enforced by the Insurance Commissioner (Utah Code § 31A-1-104; Utah Admin. Code R590-206-1).

11. ADDITIONAL AREAS OF INTEREST

Under the FIPA, government entities generally cannot request or subpoena an individual's personal financial information 'from a state or federally chartered financial institution' without either (Utah Code § 7-1-1001(2)):

- written permission from all account holders of the account referenced in the record to be examined; or
- an order from a court of competent jurisdiction.

There is an exception for certain agencies that collect records for official investigations (Utah Code § 7-1-1006(1)) if one of the exempted agencies requests a non-protected record from a financial institution, the institution may not inform the account holders referenced in the record (Utah Code § 7-1-1006(4)). When the Government obtains a record, it is obligated to reimburse the financial institution for the 'costs reasonably and directly incurred in searching for, reproducing, or transporting' the record (Utah Code § 7-1-1004(1)). A financial institution is not liable to those referenced within the records it discloses provided it reasonably believes the government's subpoena, order, or request is properly made. (Utah Code § 7-1-1007).

Further, in 2019 Utah became a leader in the area of electronic data privacy when Utah Governor Gary Herbert signed the EIDPA (Utah Code § 77-23c-101.1 et seq.). Although not specific to the financial sector, EIDPA establishes that a warrant is required when law enforcement seeks to access any data, including financial data, on electronic devices, creates a 14-day notice requirement before data subject to the warrant may be obtained, and protects subscriber records stored by electronic and computing services.

ABOUT THE AUTHORS

Lee A. Wright

Kirton McConkie

Mr. Wright is a member of the International and Corporate sections and affiliated with the Tax section. His practice focuses on franchising, licensing, manufacturing, and distribution, including disclosure and compliance. He also assists with foreign business transactions, foreign leases on property purchases, foreign independent contracts or employment

relationships, he deals with foreign governments, locates and manages foreign legal counsel, and handles overseas litigation.

Mr. Wright is a specialist in domestic and international legal data privacy issues, having been certified as a CIPP/US privacy professional. He is recognised as one of Utah's Legal Elite for International law and as a Mountain States Super Lawyer Rising Star for franchising.

lwright@kmclaw.com

Kyle Harvey

Kirton McConkie

Mr. Harvey is a member of the Kirton McKonkie's Corporate Section. His practice focuses on domestic and international corporate law, including business formation and planning, private securities offerings, corporate compliance, import and export law, international-related tax issues, and other general aspects of corporate law.

kharvey@kmclaw.com

RELATED CONTENT

GUIDANCE NOTE

Cambodia - Data Protection Overview

NEWS POST

Thailand: BoT and FCO sign MoU on financial services to strengthen transparency in the FinTech sector

NEWS POST

Malaysia: High Court fines GMSB MYR 450M for banking and money laundering offences

NEWS POST

EU: EBA launches consultation on RegTech, focuses on compliance with AML/CFT and cybersecurity requirements

NEWS POST

Nigeria: Digital Rights Lawyers Initiative files lawsuit against CBN for directive to share customer data with FinTech companies