October 23, 2020

# Information Security Regulation in the Financial and Insurance Industries – U.S. and Swiss Laws

**Jacqueline Cooney**
Paul Hastings LLP

**Martin Pauli-Burckhardt**
Bank Julius Baer & Co. Ltd

**Thomas Steiner**
LAUX LAWYERS AG

# Agenda

- Introduction
- Swiss Legal Landscape
- U.S. Legal Landscape
- Operationalization of Compliance

# Introduction

Privacy+ Security Forum

# Speaker

## Jacqueline Cooney

Senior Director Privacy & Cybersecurity
Paul Hastings LLP (Washington D.C.)

- Leads team of privacy and cybersecurity consultants who support firm attorneys and clients in operationalizing privacy and cybersecurity regulatory requirements and managing risk
- Works with global companies on building compliant and sustainable privacy programs

# Speaker

## Martin Pauli-Burckhardt

Managing Director Senior Advisor
Bank Julius Baer & Co. Ltd (Zurich, Switzerland)

- IT law counsel at Bank Julius Baer, a major wealth management bank with a global reach; previously at Credit Suisse
- Focuses on data security, data privacy and outsourcing regulations in the financial industry

# Speaker

## Thomas Steiner

Partner
LAUX LAWYERS AG (Zurich, Switzerland)

- Data, privacy and technology lawyer, advising companies on Swiss and EU data protection and security law
- Focuses on regulated sectors in digital transformation, including health, insurance and finance

# Disclaimer

Our opinions are our own and not those of our firms, companies, or clients.

# Purposes & Goals

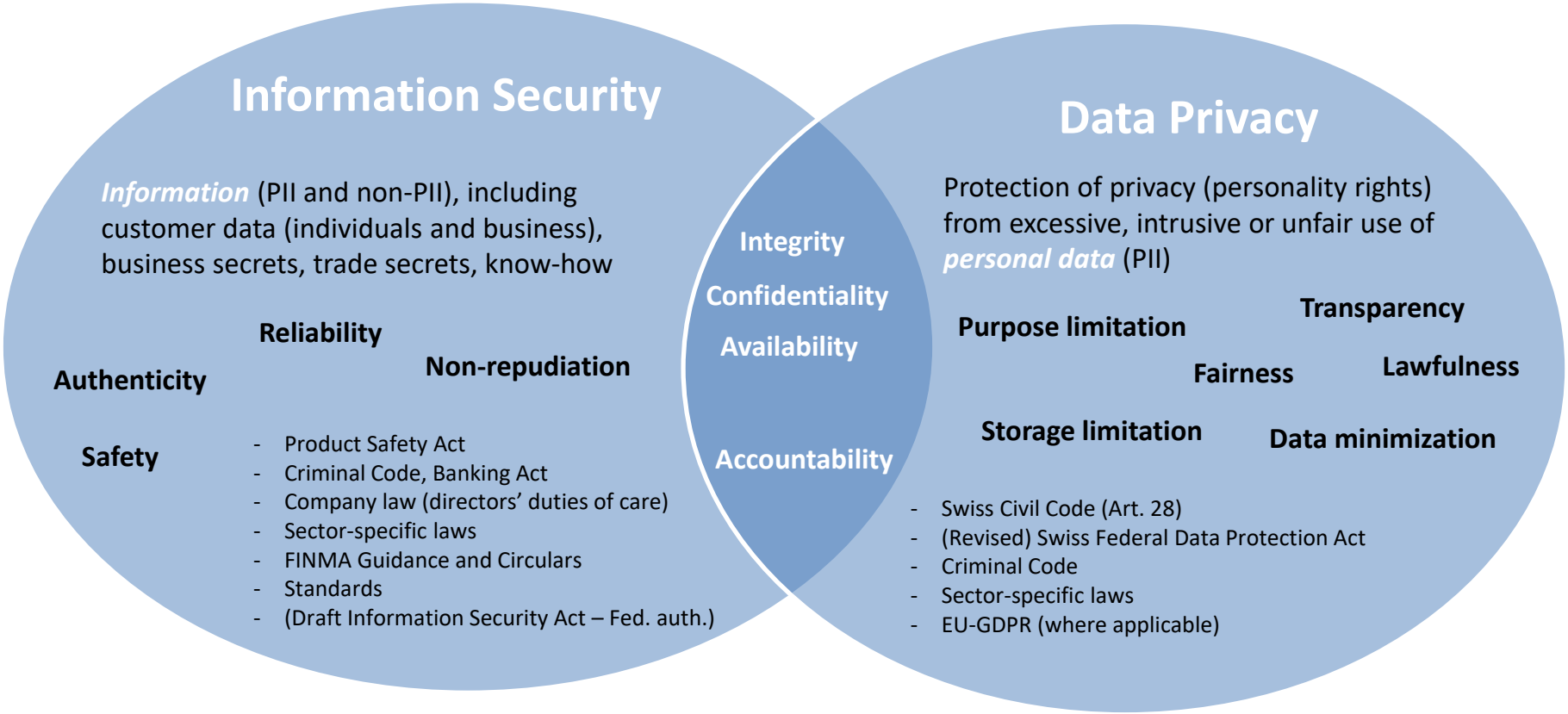
- Learn about the fragmented legal framework for information security regulations in the financial and insurance industries both in the U.S. and in Switzerland
- Consider how companies can comply with both overlapping, and at times, conflicting legal requirements for information security
- Offer practical compliance tips regarding the prevention, detection, investigation and notification of information security and confidentiality incidents, including cyber attacks

# Swiss Legal Landscape

## Overview and New Developments

Privacy+ Security Forum

# Switzerland – Overview



# New Developments – *Revised FDPA*

- Revised Swiss Federal Data Protection Act
  - Law passed on September 25, 2020 (entry into force 2022, no transition period)
  - Alignment with the EU-GDPR
- New focus on data security (integrity, confidentiality and availability of personal data)
  - **Risk-based approach**: adequacy of technical and organizational security measures commensurate with varying likelihood and severity of risks for individuals
  - **Data security breach**: new law introduces data breach notification obligations
  - **Criminal offence**: willful non-compliance with minimum data security standards (responsible natural person may be fined up to CHF 250,000; subsidiary criminal liability of company – may be fined up to CHF 10,000)

# New Developments – *Revised FDPA*

Privacy+ Security Forum

- Notification of data security breaches under Revised FDPA
  - **Data security breach**: a security breach which leads to an unintentional or unlawful loss, deletion, destruction or modification of *personal* data or to personal data being disclosed or made accessible to unauthorized persons
  - Processor to notify controller
  - Controller to notify *FDPIC* ("as soon as possible") **if breach is likely to result in high risk** to personality rights or fundamental rights of data subject
  - Controller to notify *data subject* (a) if this is **necessary for the protection of the data subject** or (b) if **FDPIC so requests**; exemptions apply (e.g. statutory duties of secrecy)
- EU-GDPR data breach notification (where applicable) – note the nuances
  - Notification of competent *EU/EEA supervisory authorities* under EU-GDPR ("within 72 hours"), **unless unlikely to result in a high risk**
  - Notification of *data subject* ("without undue delay") **if breach is likely to result in high risk** to rights and freedoms of natural persons

# New Developments – *FINMA*

- Swiss Financial Market Supervisory Authority FINMA
  - Swiss independent financial market regulator
  - Supervises banks, other financial institutions, and insurance companies
  - Mandated to protect financial market clients (creditors, investors, policyholders) and to ensure that the Swiss financial market functions effectively
  - Information security and cyber risks increasingly a focus of FINMA's supervisory activities
- FINMA's focus on information security and cyber risks
  - On-site audits by FINMA as part of regulatory audit
  - Precautionary measures:  FINMA regularly reminds institutions to identify cyber threats arising from institution-specific vulnerabilities, perform risk assessments and define countermeasures
  - Revised circulars and new guidance

# New Developments – *FINMA*

(Revised) FINMA Circular 2008/21 Operational Risks – Banks

- Banks are required to implement predefined processes in order to be able to react swiftly to confidentiality incidents concerning customer identifying information (CID), including:
  - a process for the identification of and response to confidentiality incidents;
  - adequate internal reporting that addresses the risks of confidentiality incidents;
  - a clear strategy for internal communication of confidentiality incidents;
  - with regard to *serious confidentiality incidents,* a clear (external) communication strategy; specifically addressing the form and the time of the bank's notification to FINMA, law enforcement agencies, the affected clients and the media; and
  - a framework to ensure the bank regularly reviews and continuously refines CID confidentiality and security standards and procedures.

# New Developments – *FINMA*

(Revised) FINMA Circular 2008/21 Operational Risks – Banks

- Requires cyber risk management with clear definition of tasks roles and responsibilities to,
  - identify potential institution-specific threats resulting from cyber attacks;
  - protect business processes and technology infrastructure from cyber attacks;
  - timely recognize and record cyber attacks based on processes used for systematic monitoring of technology infrastructure;
  - react to cyber attacks with timely and targeted measures; and
  - ensure timely restoration of normal business activities after cyber attack.
- Requires vulnerability tests and penetration tests
  - to protect critical and/or sensitive data and IT systems against cyber attacks
  - to be regularly performed by qualified staff with adequate resources

# New Developments – *FINMA*

Privacy+ Security Forum

- FINMA Guidance 05/2020 Duty to Report Cyber Attacks pursuant to Art. 29(2) FINMASA
  - FINMA considers risk of cyber attacks on Swiss financial institutions as “very high”, particularly in “high stress situations (such as the current COVID-19 pandemic)”
  - FINMA Guidance 05/2020 to remind supervised institutions of their obligation to “immediately report any incident [such as a cyber attack] that is of substantial importance to the supervision”
  - Focus on attacks on **critical functions** of supervised institutions, including payment trans-actions, cash supply, exchange trading, drafting and administration of insurance contracts, processing of claims and benefits, management of personal health and life insurance data
- Immediate reporting to FINMA
  - reporting to FINMA within **24 hours** of detecting a cyber attack on **critical assets** putting one or more protective goals and business processes of **critical functions** at risk
  - submission of full notification to FINMA within **72 hours**; updates in case of new developments
  - **Root cause analysis report** – more comprehensive reports in cases of attacks with severity levels “high” and “severe”

# U.S. Legal Landscape

## Overview and New Developments

Privacy+ Security Forum

# U.S. – Overview

Unlike the EU/Switzerland, US privacy laws are generally sectoral – there is no single, overarching, national law that governs privacy in the US. Financial privacy is arguably the most heavily regulated sector at the federal level with multiple laws creating a patchwork of requirements for the financial services industry enforced by several federal agencies. In addition, while many states have begun to enact more broadly applicable privacy laws in recent years, New York enacted a regulation in 2017 to specifically regulate cybersecurity practices for financial services entities.

## US Federal Laws

- Bank Secrecy Act
- Right to Financial Privacy Act
- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act
- Fair and Accurate Credit Transactions Act
- FTC Safeguards Rule

## US State Laws

Financial Services Laws:

- NY Department of Financial Services Cybersecurity Regulation

General Privacy Laws:

- California Consumer Privacy Act (CCPA)
- NY SHIELD Act
- Illinois Biometric Information Privacy Act (BIPA)
- All 50 States – breach notification laws
- Fair and Accurate Credit Transactions Act
- FTC Safeguards Rule

# New Developments

Two new developments in financial service privacy and cybersecurity regulations have impacted the way that financial services entities in the US have tackled their privacy and cyber compliance programs: 1) the proposed amendments to the FTC Safeguards Rule, and 2) the recently enacted NYDFS Cybersecurity Rule.

| | |
|---|---|
| **FTC Safeguards Rule Proposed Amendments** | • In 2019, the FTC proposed amendments to its Safeguard Rule under Gramm-Leach-Bliley. The Safeguards Rule requires financial services companies to develop, implement and maintain a comprehensive info sec program to ensure the security and confidentiality of consumer information.<br>• The proposed amendments would create more prescriptive security requirements similar to the NYDFS cybersecurity rule. Among the requirements would be encryption of data at rest and in transit, MFA, designation of a CISO, and written risk assessments.<br>• The FTC was accepting comments through August 12, 2020, and is expected to issue final regulations soon. The effective date for certain new requirements would be 6 months after publication of rule. |
| **NYDFS Cybersecurity Rule** | • In 2017, the NY Department of Financial Services published regulations requiring covered entities (NY financial services companies registered in NY) to comply with comprehensive cybersecurity requirements.<br>• Among the requirements are that covered entities must certify compliance with NYDFS.<br>• In July 2020, the NYDFS filed its first enforcement action under the NYDFS Cybersecurity Rule alleging that First American Title Insurance exposed non-public personal information (NPI) due to its failure to remediate a known vulnerability. The allegations against the Company include failure to implement several requirements, including: conducting risk assessments, maintaining appropriate data governance and classification policies, limiting user access to data, conducting regular training, and implementing certain controls, including encryption. |

# Operationalization of Compliance

Privacy+ Security Forum

# Operationalization

Privacy+ Security Forum

1. Define clear tasks, responsibilities and competencies within your organization
   - Designate privacy, cyber and incident response leads
2. Understand your data flows
   - How do you collect, store, share, protect and dispose of data?
3. Check your data practices against applicable laws and guidance
   - Jurisdictional, sectoral, applicable government agency oversight
4. Develop and implement compliant documentation
   - Review annually, audit and monitor, provide training
5. Conduct appropriate assessments (privacy, cyber, risk, IR)
   - As required by applicable law and in accordance with industry common practices

# Questions + Contact


**Jacqueline Cooney**
Sr. Director Privacy & Cybersecurity
Paul Hastings LLP
jacquelinecooney@paulhastings.com



**Martin Pauli-Burckhardt**
Managing Dir. & Sr. Advisor
Julius Baer, Zurich (Switzerland)
martin.pauliburckhardt@juliusbaer.com



**Thomas Steiner**
Partner
LAUX LAWYERS AG
Zurich (Switzerland)
thomas.steiner@lauxlawyers.ch