MAINE BANKERS Association

MONARCH ISC
INFORMATION SECURITY CONSULTING

John Hill Rogers, CISSP
john@monarchisc.com
Senior Advisor

Expo 2023

Biometrics in Banking

MONARCH ISC
INFORMATION SECURITY CONSULTING

Session Agenda

- Why Biometrics?
- Biometrics Types and Characteristics
- Biometrics Use Cases in Banking
- Biometrics in Law and Regulations
- Biometrics Challenges Vulnerabilities & Risk Considerations
- Questions & Answers

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Biometrics?

MONARCH ISC
INFORMATION SECURITY CONSULTING

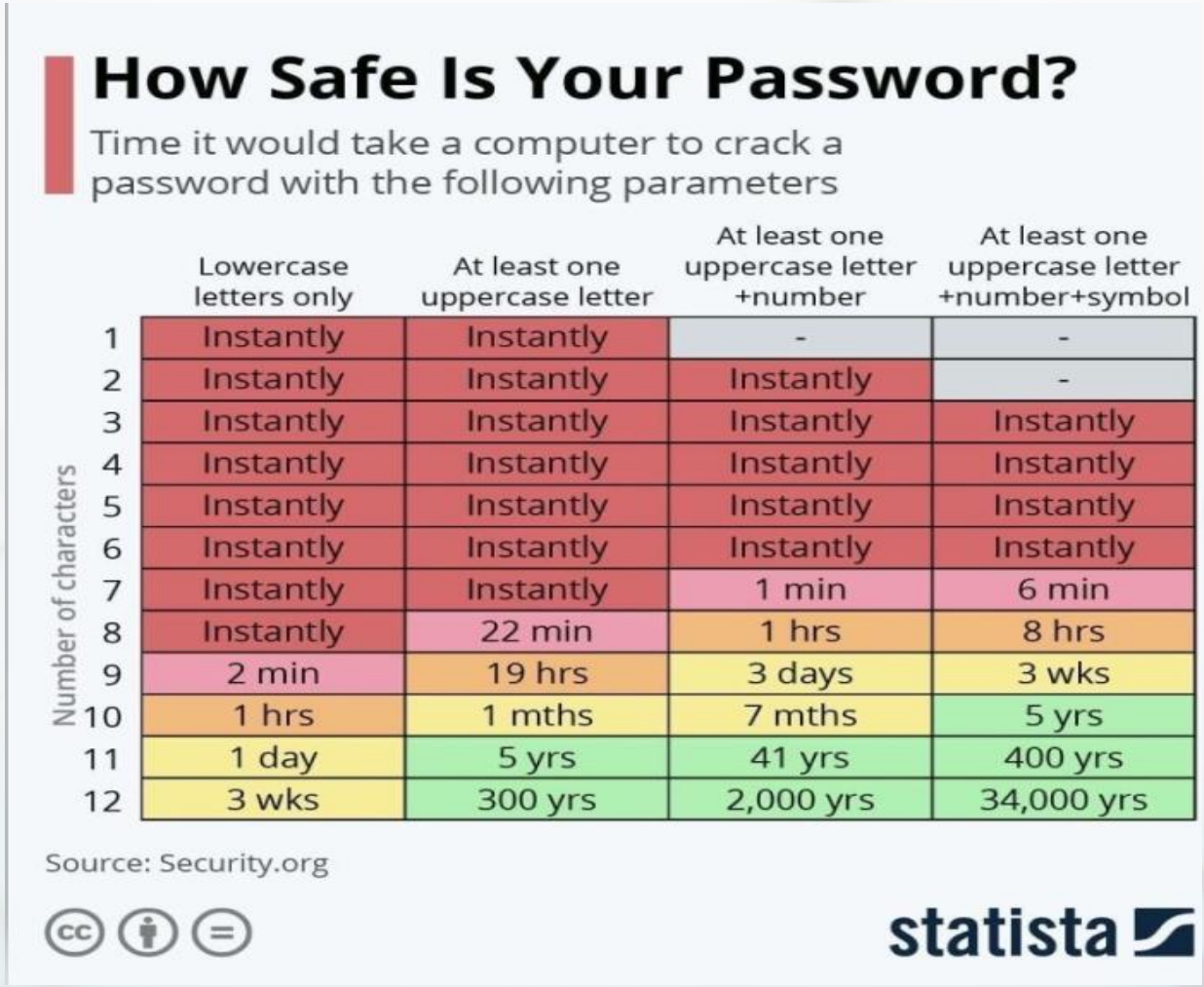
Why Biometrics?

- Regulatory push for Multi-factor authentication
  - FFIEC Access & Authentication 2021.
- Customer authentication questions
  - Negative customer experience with a reliable identity verification process.
  - Little reliable authentication with the standard verification questions.
  - Aggregate time spent on a process that does not offer a high-degree of confident identity verification.
- Help Desk password reset volume.
- Password management pain.
- Ease of authentication credential theft

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Biometrics?

- The vulnerability presented by weak passwords



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

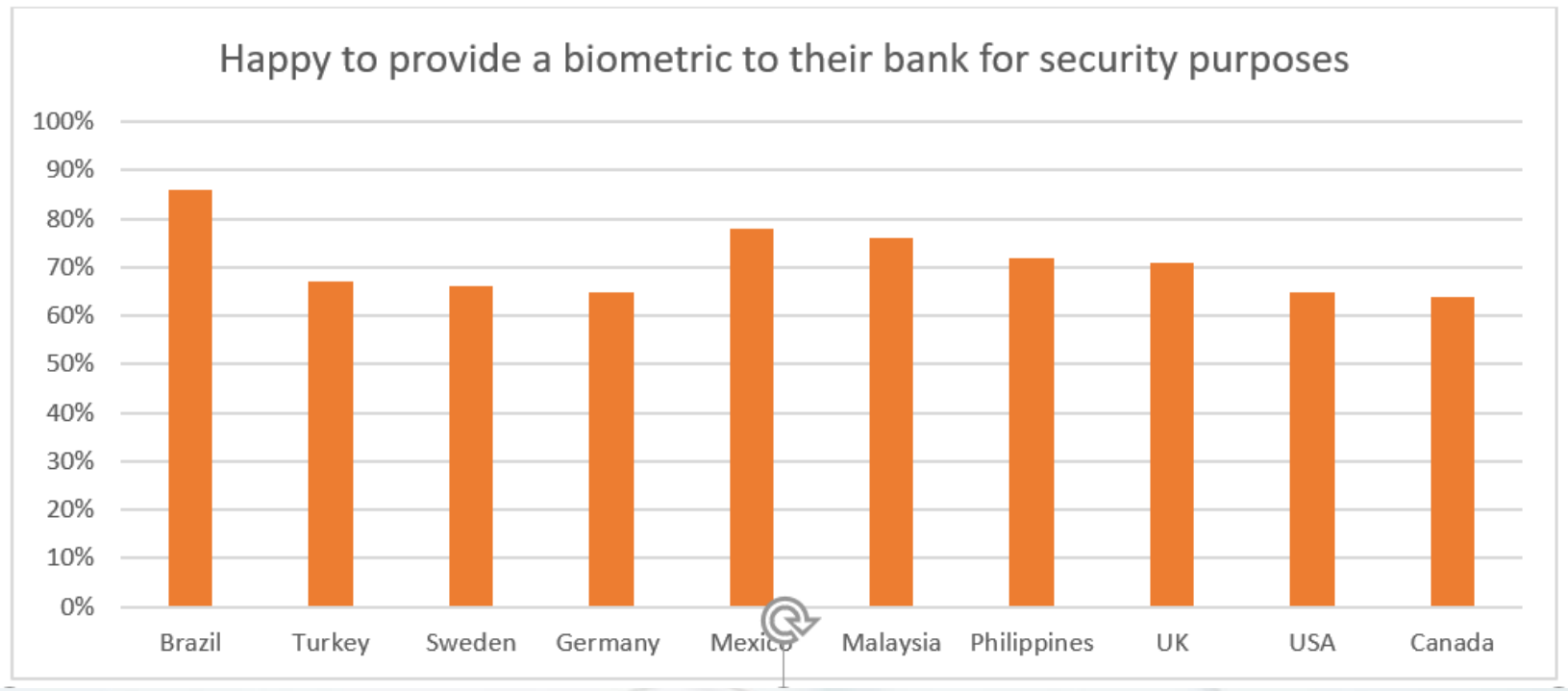
Source: Security.org

statista

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Biometrics?

- The relative popularity / acceptance of Biometrics



Independent survey of 5,000 adults carried out on behalf of FICO

MONARCH ISC
INFORMATION SECURITY CONSULTING

Why Biometrics?

- The relative popularity / acceptance of Biometrics

"A recent survey from Experian found that three in five people (61 per cent) believe 'biometric identification is either just as secure as or more secure than the current systems of passwords.'"

The Rise Of Biometric Technology In Banking (financedigest.com)

MONARCH ISC
INFORMATION SECURITY CONSULTING

Brief History

- China introduced fingerprinting in the 14th century
- Scientist Alphonse Bertillion introduces a flawed system of measuring people in ways he thought were unique and unchanging
  - Length of one foot, on leg, one finger
  - Height
- Retinal identification introduced in 1935 by Dr. Carleton Simon and Dr. Isadore Goldstein.
- Facial recognition paper published in 1971, Goldstein
- Eye Dentify Inc., in 1976
- First successful Iris recognition in 1993 at Cambridge University
- FBI installed IAFIS in 2000 with a database of 47 million fingerprints.
- Biometrics Automated Toolset (BAT) was introduced in 2001, and an accurate ID technique.

Biometric Types

MONARCH ISC
INFORMATION SECURITY CONSULTING

What are Biometrics?

Definition:

"Biometric identifier" means information generated by measurements of an individual's unique biological characteristics, including a voiceprint or imagery of the iris, retina, fingerprint, face or hand, that can be used to identify that individual.

Maine LD 1705

MONARCH ISC
INFORMATION SECURITY CONSULTING

Types of Biometrics

- Biometric Identifiers
  - Physical Identifiers
    - Fingerprint
    - Handprint
    - Face recognition
    - Iris Recognition
    - Voice recognition
  - Behavioral Identifiers
    - Typing patterns
    - Physical Movements (Gate)
    - Navigation Patterns (Mouse and trackpad)
    - Engagement patterns, including use of technology from managing applications, to our general use habits.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Biometrics Use Cases

- Biometric Use in Banking
  - Physical Identifiers
    - Fingerprint
      - Staff authentication
      - Payment authentication
      - Payment cards with embedded readers
    - Face recognition
      - Staff authentication
      - Payment authentication
      - “Selfie Pay”
    - Voice recognition
      - Call Center: Customer identity verification
  - Behavioral biometry – “Inherence factor”
    - Use patterns for customer behavior for mobile and online banking
      - Fraud detection

MONARCH ISC
INFORMATION SECURITY CONSULTING

Discussion Break:

Using Biometrics?

MONARCH ISC

Biometrics in Regulations

MONARCH ISC

Biometrics in State Regulations / Laws

- 2008 Biometric Information Privacy Act – Illinois
  - First Biometrics Privacy Law
  - Regulates the collection, retention, disclosure, and destruction of biometrics, such as fingerprints, handprints, voiceprints, eye scans, and the facial geometry characteristics captured by facial recognition systems.
  - Specifically, section 15 of BIPA outlines the obligations of private entities that collect or otherwise obtain biometrics.

- On February 17, 2023, the Illinois Supreme Court held in a 4-3 split opinion that claims under the state's Biometric Information Privacy Act (BIPA) accrue each time there is a biometric collection or transmission constituting a potential violation, even if the same biometric identifier is being collected or transmitted by the same entity from the same individual repeatedly. This opinion follows a recent Illinois Supreme Court decision that found a five-year limitations period for BIPA claims.
- Companies should take note that these two rulings in combination could mean that they are vastly more exposed to litigation risk than previously anticipated. For example, a company that uses a fingerprint scanning system to track employee attendance that is not BIPA-compliant may be liable for every fingerprint scan going back five years, with the potential for penalties up to $5,000 per violation.

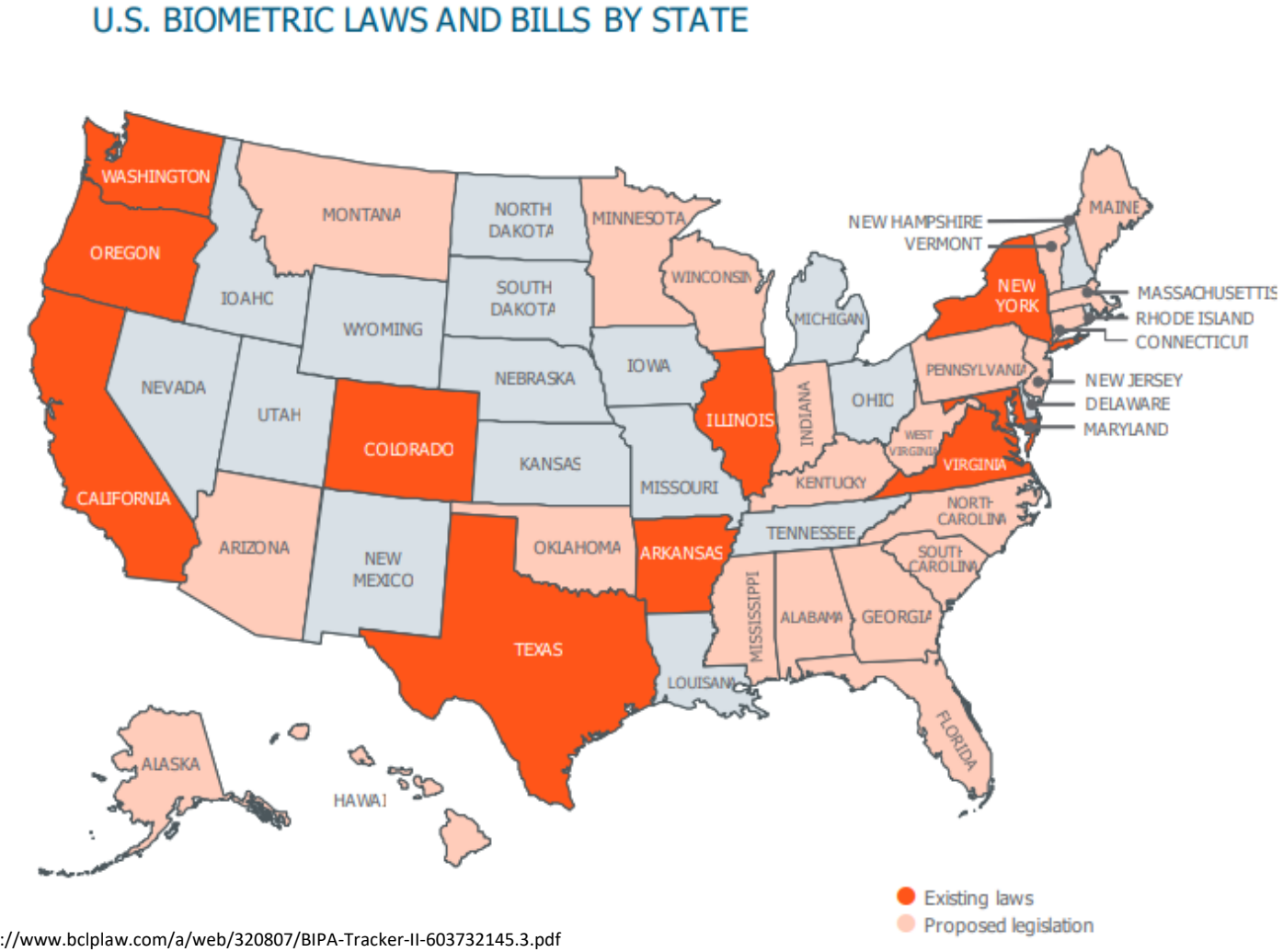
MONARCH ISC
INFORMATION SECURITY CONSULTING

Biometrics in State Regulations / Laws

- 2023 – Maine LD 1705 - An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data.
  - “This bill provides for an individual's privacy regarding the collection and use of biometric identifiers of the individual and personal information connected to the biometric identifiers. The bill requires a written release from an individual before a private entity may obtain or use biometric identifiers and requires the private entity to establish a policy for retention and destruction of the biometric identifiers. The bill provides for a private right of action for an aggrieved individual who has had biometric identifiers obtained or used in violation of the provisions related to biometric identifiers, as well as civil penalties and enforcement by the Attorney General. The bill also provides that violations of provisions related to biometric identifiers constitute violations of the Maine Unfair Trade Practices Act.”
  - Referred to Committee on April 20, 2023
  - Public hearings not yet scheduled
  - MaineBankers seeking to exempt Maine’s Banks at “entity-level” from new state privacy regulations.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Biometrics in State Regulations / Laws



https://www.bclplaw.com/a/web/320807/BIPA-Tracker-II-603732145.3.pdf

MONARCH ISC
INFORMATION SECURITY CONSULTING

Biometrics in Federal Regulations / Laws

- Bill Only: National Biometric Information Privacy Act of 2020.

- This bill requires a private entity that obtains an individual's biometric identifier or biometric information to take specified actions to maintain and ensure the privacy and security of such biometric data.
- Must have…written policy establishing a retention schedule and guidelines for destroying such data on the earlier of
  - (1) the date on which the initial purpose for collecting the data has been satisfied.
  - (2) one year after an individual's last intentional interaction with the entity.
- Must require data to provide service.
- Must inform individual in writing of the collection
- A private entity may not obtain an individual's biometric data unless
  - (1) the entity requires the data to provide a service or for a valid business purpose, and
  - (2) the entity informs the individual in writing of the collection and its purpose and receives a written release.
  - Further, a private entity in possession of such data may not sell, lease, or otherwise profit from the data.
  - A private entity must store, transmit, and protect from disclosure all biometric data in its possession in a manner that is the same as, or more protective than, the manner in which the entity treats other confidential and sensitive information. Upon request, the entity must disclose to an individual such data relating to the individual collected during the preceding 12 months.
- Further, the bill establishes a private right of action for any individual aggrieved by a violation of the bill's provisions.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Biometrics in International Law

EU General Data Protection Regulation (GDPR)

- The GDPR prohibits the processing of biometric data for the purpose of uniquely identifying natural persons.
- The exemptions the GDPR provides are limited and very restrictive. Individual's explicit consent is an example of an exemption.
- Note that in an employer-employee relationship explicit consent cannot be used as an exemption due to the imbalance between the controller and the data subject. It is deemed that consent cannot be freely given in such case.

Challenges & Risk Considerations

MONARCH ISC

Authentication vs. Verification

Authentication	Verification
Authentication refers to a process of determining that an individual is who only they claim to be.	Verification means ensuring that the data is associated with a particular individual.
For example, asking dynamic Knowledge-Based Authentication questions that would be difficult for a different individual to answer. Generally, to access bank statements you need to enter the account number as a password.	For example, you are matching address or date of birth to an individual's name.
For authentication, the individual has to answer specific questions to find out whether that person or individual is eligible to have certain rights to access this resource or not.	For verification, the given data which is entered by an individual is matched with the previously stored information present in the database.
Authentication takes confirmation to the next level and is especially important when we are dealing with online transactions.	Verification alone is required by some businesses and is merely an extra layer of security for others.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Biometrics Challenges

- User assent to have stored biometric data.
- Inconsistency with some human fingerprints has caused significant issues in enterprise adoption of biometrics using finger scans.
- System integration between third-party biometric systems and Windows Hello or Apple FaceID.
- Latency / delay in processing facial scans.
- “Live human” controls difficult to tune to prevent static images being used to authenticate.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Biometrics Vulnerabilities

- Thumbprints have been spoofed with the type of gelatin used in Gummi Bears and a picture of someone else's thumb.
- A journalist and his twin hacked HSBC's phone banking voice ID system — though it wasn't easy.
- Facial recognition systems can be foiled by deepfakes, masks, and virtual reality — and they often show racial bias.
- Voice recognition vulnerable to site like resemble.ai
  - Unknown callers / social engineers recording voices of their victims and using this site to record new statements with that “voiceprint”.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Attacks in Biometrics

- **Fake Biometric:** Hackers give a fake biometric sample to a sensor to get access to the biometric system. Fake face masks, false fingerprint made from silicon, the lens on an iris, etc. are few such malicious attacks on the sensor.
- **Replay Attack**: In this attack, the data stream which is contained in the biometric system is injected between the sensor and the processing system.
- **Template Tampering Attack**: A template represents a set of salient features that summarizes the biometric data (signal) of an individual. The templates can be modified to obtain a high verification score, no matter which image is presented to the system. The templates which are stored in the database can be replaced, stolen or even can be altered. Thus, bringing the system down by making the score low for legitimate users. The template-generating algorithms have been viewed as one-way algorithms.

https://www.javatpoint.com/biometric-system-security-and-attacks

Attacks in Biometrics

- **Overriding Yes/No response**: The result of the system is always a binary response, Yes/No (i.e., either match/no match). In other words, there is still a fundamental disconnecting between the biometric and applications, which make the system, open to potential attacks.
- **Trojan horse attack**: In Trojan horse attack the feature extractor is itself replaced to produce the desired features and to add on those features in the existing database. The spoof detection technology has become a crucial part of a biometric system as with an increasing concern for security, the biometric attacks are to be identified, controlled and minimized. Researchers are developing various new approaches for a secure biometric system.
- **Masquerade attack**: It was demonstrated that a digital "artifact" image could be created from a fingerprint template so that this artifact is submitted to the system, will produce a match. The object may not even resemble the real image. This attack poses a significant threat to the remote authentication machines. Since a hacker does not even have to bother to obtain a valid biometric sample, all he needs is to get access to the templates stored on a remote server.

Recap

- Biometrics are fast becoming standard expectation for users.
- Banks increasing adoption to solve the customer service vs security problem.
- Banks adopting internal biometrics for user authentication to solve the help-desk / password management problem
- States are passing privacy laws with significant penalties.
- Case law is accumulating.
- Biometric vulnerabilities must be carefully considered and controlled.
- Adequately hardened networks and systems become more critical, along with detective control adequacy.

MONARCH ISC
INFORMATION SECURITY CONSULTING

MAINE BANKERS Association

Questions?

Thank you!

John Hill Rogers, CISSP
Senior Advisor
john@monarchisc.com
www.monarchisc.com

MONARCH ISC

References

1. https://www.financedigest.com/the-rise-of-biometric-technology-in-banking.html
2. https://www.securitymagazine.com/articles/98506-banking-and-behavioral-biometrics-understanding-privacy-and-security-regulations
3. https://www.axios.com/2020/02/18/biometrics-banking-retail-privacy
4. https://www.techtarget.com/searchsecurity/definition/biometric-payment
5. https://www.biometricupdate.com/202111/using-and-storing-biometric-data-scrutinizing-practices-of-banks-and-governments
6. https://iopscience.iop.org/article/10.1088/1742-6596/1964/6/062109/pdf
7. https://www.fico.com/blogs/four-ways-biometrics-will-evolve-banks
8. https://www.recogtech.com/en/knowledge-base/5-common-biometric-techniques-compared
9. https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html
10. https://www.javatpoint.com/biometric-system-security-and-attacks#:~:text=Biometric%20system%20has%20various%20limitations,while%20designing%20the%20biometric%20system.
11. https://legislature.maine.gov/legis/bills/display_ps.asp?LD=1705&snum=131
12. https://www.bclplaw.com/a/web/320807/BIPA-Tracker-II-603732145.3.pdf
13. HSBC's phone banking voice recognition security hacked (computing.co.uk)

MONARCH ISC
INFORMATION SECURITY CONSULTING