Kennebec Savings Bank

150 State Street | P.O. Box 50 | Augusta, Maine 04332 | Telephone: (207) 622-5801

October 17, 2023

Testimony to the 131st Maine Legislature
Committee on Judiciary

Good afternoon, Senator Carney, Representative Moonen, and honorable members of the Joint Standing Committee on Judiciary. My name is Craig Garofalo, and I am the Executive Vice President and Chief Operating Officer at Kennebec Savings Bank. I am testifying today in opposition to L.D. 1977, *An Act to Create the Data Privacy and Protection Act* and L.D. 1705, *An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data*.

As a community bank, the trust our customers and fellow community members place in us to protect their information and financial assets is central to what we do every day, and I appreciate the opportunity to speak with you all today.

To help our customers protect themselves against constantly evolving online threats, we use a variety of technological tools to build and maintain a safe and secure environment. Some of these tools may use biometric identifiers like voice recognition, fingerprints, or face recognition. Use of these identifiers as part of a holistic security program is safer than the use of passwords alone, and helps us ensure the level of cyber security that customers expect, deserve, and in many cases demand.

I am concerned that this legislation would restrict our ability to use biometric identifiers in our ongoing efforts to keep customer data secure. Bad actors attempting to attack and exploit our customers online are constantly evolving and enhancing their methods to get around the measures we work with our customers to implement. I worry that an entire category of security technologies that are simple to use, and highly in demand from our customers and community members, would be less accessible or unavailable entirely.

I understand the apprehensions that many have about how customer data, including biometric data, is used, and I am glad that strong consumer advocates are speaking out to make sure businesses and industries are held to a high standard. With that said, we do not currently store this biometric data in our systems.

As a bank, our privacy practices are already subject to robust scrutiny. Because of the sensitivity and importance of the data needed to serve our customers, banking is one of the most heavily regulated industries in the country. We are subject to strict requirements for storage, protection, use, and nondisclosure of customer data, and our ability to continuously meet or exceed those standards is examined regularly by independent enforcement agencies at the state and federal level. The protections and requirements of existing law, including the Gramm-Leach-Bliley Act, are designed to be broad, protecting ALL forms of nonpublic customer information. Whether the data is account information, personal details, biometric identifiers, or any other form of data that might emerge in the future, our obligations are clear, substantial, and heavily examined.

I would ask the Committee to support a full entity-level exemption for financial institutions already subject to the requirements of the Gramm-Leach-Bliley Act. I believe an exception would preserve the clarity and high standards of existing law and help create a coordinated approach moving forward.

In conclusion, I urge a thoughtful and comprehensive approach as you consider the options available to meet our shared goal of protecting our community members, and our customers.

Thank you for your consideration, I am happy to answer any questions.

Respectfully Submitted,

Craig Garofalo

Why Banks use Biometrics:

Banks obtain and retain a significant amount of valuable assets and confidential information. Cybercriminals around the world are relentless in trying to obtain access to misdirect funds and steal identities. Regulators require banks to deploy suitable controls adequate to prevent unauthorized access to accounts and information. Banks are strongly recommended to use Multi-Factor Authentication (MFA), whenever possible. To comply with MFA standards, access is only granted when an individual can provide evidence from at least 2 factors of the following 3 factors listed below.

● Something you know: i.e., username, password, ID number, PIN, date of birth, mother's maiden name, etc.
This is the least reliable as these items can be easily stolen, memorized, or guessed.

○ Something you have: i.e., physical items: keys, badge, card, USB, one-time password sent to a device, etc.
This is moderately reliable as these items can be stolen, replicated or intercepted.

● Something you are: i.e., Biometrics: voice, retinal, face, fingerprint recognition.
This is the most reliable as these cannot be replicated.

It's important to note that supplying multiple items from only one of the factors above **DOES NOT** comply with MFA standards.

How Biometrics are used:

Mobile and remote access

Access to most banking apps can be controlled through biometric identification tools installed on an individual's personal devices (i.e., cellphone, tablet, laptop). Most banking apps will allow the use of "Face Id" to open and access their accounts from a personal device. Essentially, the bank is asking the device to authenticate the user on the bank's behalf. If the device recognizes the user's face, it authorizes the bank to open the app. At no time during this process does the bank receive any data about the user's face or their biometrics. It simply receives authorization and approves access based on the device's controls.

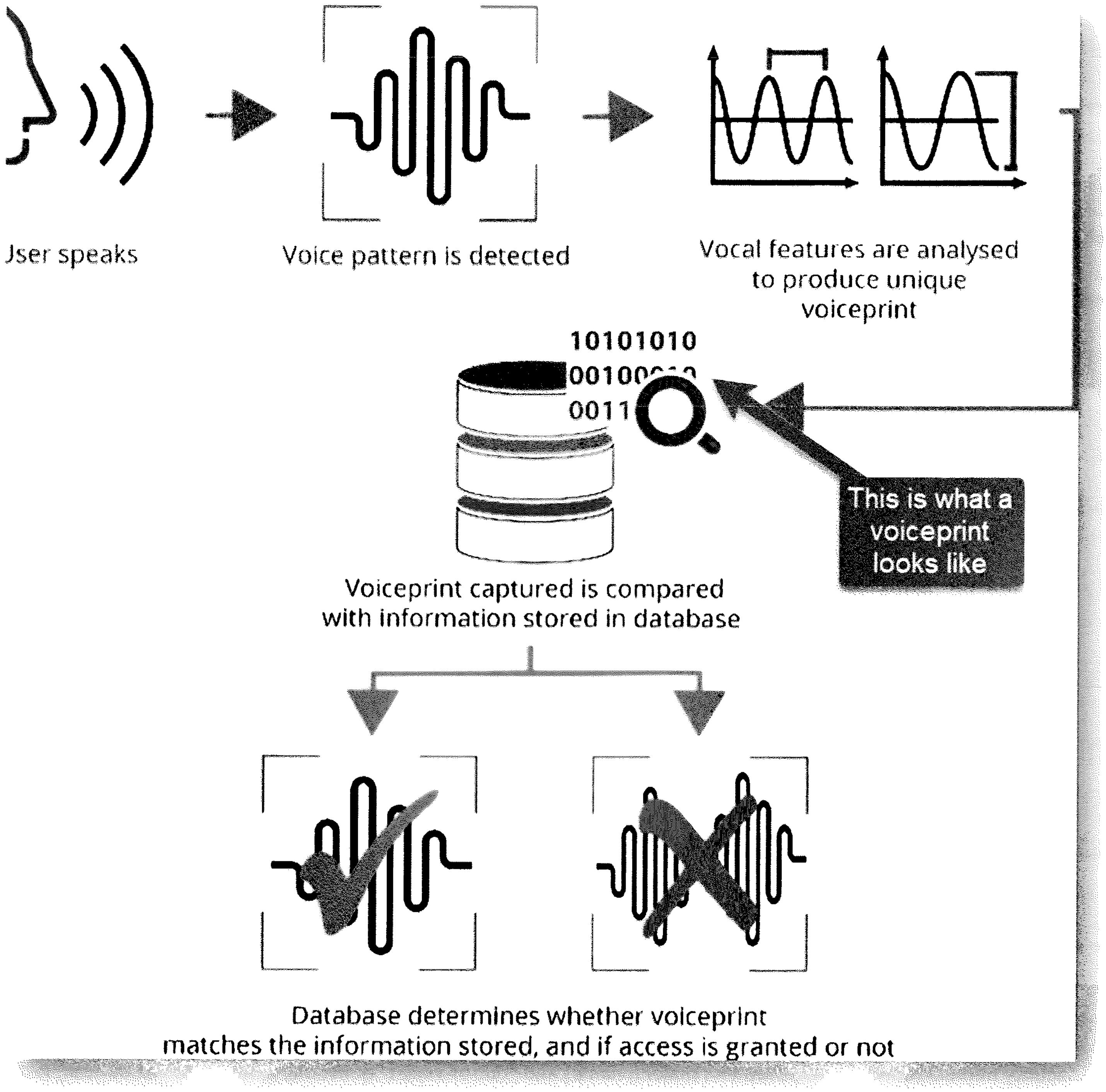
Call centers

Many banks are using Voice ID to authenticate customers when they call in to access information about their account or conduct financial transactions. When a customer opts into Voice ID, their voice is analyzed and stored as a numeric data file. It's important to understand, the data file created is NOT a recording. It's a series of data points that uniquely describes the person's voice in manner that allows a software to compare it to future phone calls. This process provides a reliance factor of voice on the line and authenticates the caller as the legitimate user of the account. The data file created is unique and essentially unusable outside of this environment; meaning it cannot be reversed engineered to create a customer's voice. *(See Exhibit A on the back for a visual depiction of Voice ID)*

Acceptance of Voice ID

Prior to Voice ID, our Bank attempted to authenticate callers by asking a series of "identification questions" (social security number, date of birth, mother's maiden name) and "out-of-wallet" questions (amount of last deposit, last check written, branch where the account was opened). Failure to answer questions accurately resulted in asking more difficult questions or ultimately sending the customer to the nearest branch. Due to data breaches like Equifax and the plethora of information for sale on the dark net, cybercriminals around the world are now more equipped to answer these questions than our actual customers. In June 2020, we introduced Voice ID to our customers. To date, over 93% of our callers have opt-ed into the Voice ID program (which exceeds the National average of 90%). Of our declines, most were one-time callers that felt it wasn't necessary or didn't have the time to sign up. Only about ½ of a percent of declines voiced concerns about privacy. To date, we have over 105,000 customers enrolled in the program. We've intercepted over 300 fraudulent attempts to access legitimate customer enrolled in Voice ID. From those cases, we created a watchlist of 85 confirmed fraudulent voices. This means that those 85 individuals cannot defraud any of our customers again without our system detecting them.

Exhibit A – Voice ID


Jser speaks
Voice pattern is detected
Vocal features are analysed to produce unique voiceprint
10101010
00100
0011
This is what a voiceprint looks like
Voiceprint captured is compared with information stored in database
Database determines whether voiceprint matches the information stored, and if access is granted or not

Andrew Grover, CPA, CFE, CISA, CITP
Executive Vice President and Chief Risk Officer for Bangor Savings Bank.

Andrew is a Certified Public Accountant, Certified Fraud Examiner, Certified Information Security Auditor and Certified Information Technology Professional. Andrew is responsible for providing oversight and guidance for the Bank's enterprise risk management program. Andrew has over fifteen years of community banking experience in Maine specializing in enterprise risk management, anti-money laundering, financial crime investigations, information and cyber security, and legal and regulatory compliance.