Pindrop®

FAQ

Pindrop and the FFIEC Authentication Guidance

How Pindrop® solutions can help you secure authentication that follows the FFIEC way

Pindrop® solutions, as detailed below, offer the functionality to help financial institutions to reduce risk, foster consumer protection and bolster FFIEC-required "safety and soundness" efforts as they develop, implement and maintain the risk controls to address the factors identified by the Federal Financial Institutions Examination Council's (FFIEC) guidance "Authentication and Access to Financial Institution Services and Systems" issued in August 2021 (the "Guidance").

DISCLAIMER: This FAQ document does not, and is not intended to, constitute legal advice or the provision of legal advice for or on behalf of Pindrop or any third party. Any customer or potential customer of Pindrop is responsible for ensuring that it obtains its own legal advice.

Overview

	Practices and Controls Identified by the FFIEC	Pindrop Solutions
 **Authentication Solutions**	**Device Identification and Enrollment.** Unique identifiers or characteristics of the caller's device are identified and used to authenticate by obtaining a complex digital "fingerprint" of the device or by other secure identification techniques. Some device identifiers, such as device cookies, geo-location, and Internet Protocol (IP) address matching, are considered insecure and ineffective if used alone, but can be combined with other controls for additional protection.	Pindrop solutions use a multi-factor authentication system that includes the analysis of a caller's device (Something You Have) to help FIs authenticate and enroll genuine customers.
	Behavioral Biometrics Software. Software analyzes the behavioral biometrics or characteristics of a customer, such as the customer's interaction with a mobile phone or other access device, to authenticate the customer. Behavioral biometric analysis can include data such as the customer's finger swipes, taps, keystrokes, and mouse usage.	Pindrop solutions analyze characteristics of customer interaction with a device via the keypresses (such a tone of a keypress or how quickly the keys are pressed) as one factor to help an FI determine whether to authenticate the caller against an enrolled profile.
 **Customer Call Centers and IT Help Desk Controls**	**Identify Unauthorized Access Attempts.** Controls identify deviations from a customer's or user's usual geographic location or method of communication for the account, such as an Internet-based communication application or an unidentifiable phone number.	Pindrop solutions analyze the phone number, telco signaling data, and acoustical elements of a call to help FIs determine whether to authenticate a caller against an enrolled profile.

	Practices and Controls Identified by the FFIEC	Pindrop Solutions
 **Transaction Logging and Monitoring Controls**	**Fraud and Anomaly Detection Monitoring.** Processes designed to detect fraud and other anomalies, such as changes in user or customer behavior, transaction velocity and increases in login or account lockout activity. These processes can also provide a timely alert to management to unauthorized access and/or potential fraud.	Pindrop solutions feature real-time fraud, risk and anomaly detection functionality along with case management and batch reporting operationalization capability.
	Suspicious Behavior Monitoring. Processes monitor and report customer and user access, especially privileged and remote access users, for suspicious behavior.	Pindrop solutions use a variety of factors to help identify suspicious calling behavior and report suspicious activity to FI customers in both real-time and via batch reports.
	Fraud Response Policies. Response policies address situations where customer or user devices are identified as potentially compromised and where customers or users may be facilitating fraud.	The policy manager functionality in Pindrop solutions enable FI customers to configure their own risk-based policies and use the outputs from such solutions to write customer defined response/ mitigation procedures that best fit the customer's business needs.
	Monitoring and Reporting of Unauthorized Access by Third Parties. Processes are in place for FI third-party service providers to report, and the FI to log and monitor unauthorized access to critical outsourced systems.	Pindrop's solutions can be used as a tool to assist our FI customers in establishing appropriate internal policies, procedures and processes for the FI to log and monitor access to its critical systems.
 **System and Network Design and Architecture Controls**	**Endpoint / Device Authentication.** Controls are in place to ensure only authorized devices can connect to the FI's information systems, networks, or services.	Pindrop solutions use a variety of analytics-driven mechanisms such as network analytics, Phoneprinting® Technology and Toneprinting® to verify, enroll and identify phone devices as a tool to help enable FIs to limit access to accounts and information only by authorized devices.
	Device Blocking or Network Indicators. Connections to the financial institution's systems or servers are blocked based on devices, networks, or IP addresses known or suspected to be associated with fraudulent or malicious activities.	ANI blocklisting and telco network analytics are examples of functionality that Pindrop solutions offer to enable our FI customers to identify potential suspicious devices, discover fraudulent behavior and act to address malicious activities and help foster protection of their customers.

FAQ

Can a financial institution ("FI") use Pindrop's solutions to help achieve compliance with the Guidance?

Yes. The Guidance reinforces the need for FIs that use Internet or mobile cellular network communications for providing customers with banking services or transactions to effectively authenticate users and customers as part of their information security program. Key risks and considerations for FIs to tackle include:

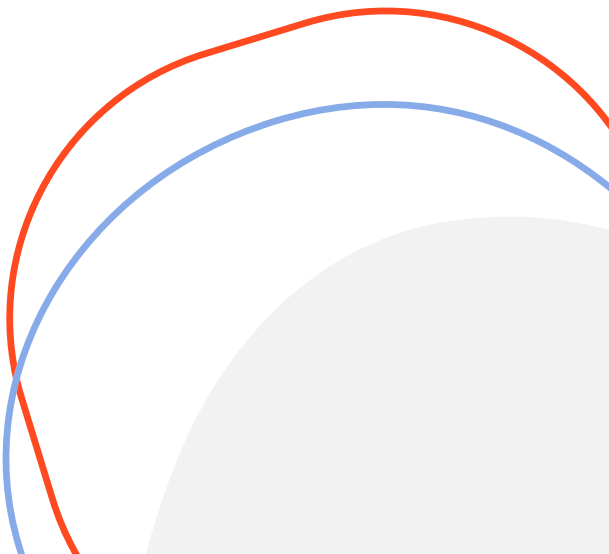
- The more extensive cybersecurity risk landscape necessitating layered security;[1]
- The significance of risk assessments and effective risk assessment practices, such as measures to identify users that may pose higher risks or even outright threats that can help FIs to augment appropriate internal access and authentication practices;[2]
- The increasing threat posed by certain digital banking services, such as push payment and password cracking tools, particularly with respect to older systems;[3]
- The weakness of single factor authentication and the value of biometric identifiers;[4]
- The importance of monitoring, activity logging, and reporting processes and controls;[5]
- The existence of bad actors focused on social engineering techniques and call center weaknesses and the usefulness of risk mitigation tools to establish effective call center controls and combat threat actors;[6] and
- The importance of reliable identity verification methods.[7]

1. Id. Introduction/Sections 1 and 2, pages 1-3.
2. Id. Section 3, page 4-6.
3. Id. Section 3, p. 5.
4. Id. Section 5, pages 6-8.
5. Id. Section 6, page 8.
6. Id. Sections 7 and 8, page 8.
7. Id. Section 11, page 10.

How can Pindrop's solutions help mitigate the key risks and considerations highlighted in the Guidance?

Pindrop's solutions are designed to provide the opportunity for financial institutions to create multi-layered security controls to address potential weaknesses in any one control and help a financial institution mitigate the key risks and address the considerations highlighted in the Guidance. Examples include:

- Layered approach to security. Pindrop solutions use a multi-factor authentication approach, including voice (Something You Are), device (Something You Have), network analysis (Something You Have), behavior-keypress analytics (Something You Are) and other factors such as risk to help FIs to identify potential fraudsters and to give FIs additional tools to help them verify genuine customers.
- Pindrop's approach also provides both preventative and detective controls in the form of account monitoring analytics and fraud detection.
- Pindrop's voice-authenticity controls can be integrated as an additional layer of security used to mitigate attacks.
- Reliable identity verification methods. Pindrop's solutions offer a mechanism for FIs to help them verify genuine callers against enrolled profiles and reduce the risk of identity theft, as part of an FI's customer's identification program and in compliance with FI customer due diligence expectations.
- Ability to help the institution monitor, log activity, and report potential suspicious activity. Pindrop offers solutions that provide account risk analytics based on call data that help identify when suspicious activity on an account may have occurred.
- Innovative alternative to the traditional password. The availability of tools that threat actors exploit that circumvent traditional methods of authentication (like push payments or passwords) pose significant risks and reinforce the need for FIs to effectively authenticate users and FI customers to protect information systems, accounts, and data. The features and functionality of the Pindrop solutions are designed to achieve these objectives.
- Bad actors focused on social engineering and call center weaknesses. Pindrop's call center authentication and fraud solutions are uniquely positioned to address manipulative social engineering techniques, such as by leveraging its Deep Voice™ engine to help identify potential fraudsters. The Guidance identifies the use of voice as a methodology for enhanced authentication control.[8]
- Assist with an institution's operationalization of risk assessments. Pindrop solutions can help mitigate risks surfaced in connection with existing authentication practices, serving as a control against security threats to reduce residual risk to the FI and costs associated with corrective actions.



8. Id. Section 2, p. 3 and Appendix, p. 12.

Does the Guidance identify specific practices and controls FIs should adopt?

Yes. The Guidance's Appendix notes examples of specific practices and controls related to access management, authentication, and supporting controls that FIs can use to reduce such risks and execute included recommendations. The chart above illustrates how Pindrop's solutions are designed to help FIs operationalize many of these practices and controls.

Why is it important to consider solutions like those offered by Pindrop to help comply with the Guidance?

While the FFIEC itself does not itself have any enforcement authority, the regulators comprising its board of governors, including the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Consumer Financial Protection Bureau refer to FFIEC standards, handbooks and guidance when performing examinations. If a regulator is engaged in an audit, examination or investigation or pursuing a complaint, it may look to compliance with the Guidance as evidence of the reasonableness of the actions taken by the FI. Moreover, the failure of an FI to implement appropriate controls may expose the institution to potential loss from fines and penalties issued by its primary regulator as well as from consumer litigation.[9]

9. Information Technology Examination Handbook, Federal Financial Institutions Examination Council.

About Pindrop

In an increasingly digital world, Pindrop® lets people use their voice to seamlessly connect to, enter and unlock new experiences while safeguarding their privacy. Using its patented precise voice identification technology, Pindrop is leading the way to the future of voice by establishing the standard for identity, security, and intelligence for voice interactions. Protecting some of the world's biggest banks, insurers and retailers, Pindrop enables customers to quickly, conveniently and securely connect to the information and resources they need. Its precise voice identification technology recognizes unique identifiers within the human voice that enables its customers to prevent fraud and deliver exceptional customer experiences in call centers, obtain information from smart devices and even activate cars. A privately held company, Pindrop is venture-backed by Andreessen Horowitz, Citi Ventures, Felicis Ventures, CapitalG, GV, IVP, and Vitruvian Partners. Visit pindrop.com for more information.

Follow us

Pindrop @PindropSec @Pindrop @Pindrophq pindrop.com

Pindrop®