Department of Financial Services

Industry Guidance

Industry Letter

To: The executives and information security personnel at all entities regulated by the New York State Department of Financial Services ("DFS" or "the Department")

Re: Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks

Date: October 16, 2024

Introduction

The advancements in artificial intelligence ("AI") and increased reliance on AI has had a substantial impact on the cybersecurity landscape as this technology has introduced significant new opportunities for cybercriminals to commit crimes at greater scale and speed.[1] AI also has positively impacted cybersecurity, improving the ability of entities - including those regulated by DFS (referred to herein as "Covered Entities") - to prevent cyberattacks, enhance threat detection, and improve incident response strategies.[2]

The Department has received inquiries about how AI is changing cyber risk and how Covered Entities can mitigate risks associated with AI. The Department is publishing this guidance in response to those inquiries and in accordance with its mission to protect New Yorkers and New York businesses from cybersecurity risks. It is intended to be a tool to assist Covered Entities in

understanding and assessing cybersecurity risks associated with the use of AI and the controls that may be used to mitigate those risks. This Guidance does not impose any new requirements beyond obligations that are in DFS's cybersecurity regulation codified at 23 NYCRR Part 500 (the "Cybersecurity Regulation" or "Part 500"); rather, the Guidance is meant to explain how Covered Entities should use the framework set forth in Part 500 to assess and address the cybersecurity risks arising from AI.

Risks

While there are many risks related to the use of AI, there are certain threats that are specific to cybersecurity. This Guidance highlights some of the more concerning threats identified by cybersecurity experts, but they are not exhaustive. The first two are risks caused by threat actors' use of AI, while the latter two are risks caused by a Covered Entity's use or reliance upon AI.

AI-Enabled Social Engineering

AI-enabled social engineering presents one of the most significant threats to the financial services sector. While social engineering has been an issue in cybersecurity for years, AI has improved the ability of threat actors to create highly personalized and more sophisticated content that is more convincing than historical social engineering attempts. Threat actors are increasingly using AI to create realistic and interactive audio, video, and text ("deepfakes") that allow them to target specific individuals via email (phishing), telephone (vishing), text (SMiShing), videoconferencing, and online postings.[3] These AI-driven attacks often attempt to convince employees to divulge sensitive information about themselves and their employers. When deepfakes result in the sharing of credentials, threat actors are able to gain access to Information Systems containing Nonpublic Information ("NPI").[4] In addition to disclosing sensitive information, AI-driven social engineering attacks have led to employees taking unauthorized actions, such as wiring substantial amounts of funds to fraudulent accounts.[5] Further, deepfakes have been used to mimic an individual's appearance or voice in an attempt to authenticate that individual and circumvent biometric verification technology.

AI-Enhanced Cybersecurity Attacks

Another major risk associated with AI is the ability of threat actors to amplify the potency, scale, and speed of existing types of cyberattacks. As AI can scan and analyze vast amounts of information much faster than humans, threat actors can use AI quickly and efficiently to identify and exploit security vulnerabilities, often allowing threat actors to access more Information

Systems at a faster rate. Once inside an organization's Information Systems, AI can be used to conduct reconnaissance to determine, among other things, how best to deploy malware and access and exfiltrate NPI. Furthermore, AI can accelerate the development of new malware variants and change ransomware to enable it to bypass defensive security controls, thereby evading detection.

In addition, AI has accelerated the speed and scale of cyberattacks. With the increased proliferation of publicly available AI-enabled products and services, it is widely believed by cyber experts that threat actors who are not technically skilled may now, or potentially will soon, be able to launch their own attacks. This lower barrier to entry for threat actors, in conjunction with AI-enabled deployment speed, has the potential to increase the number and severity of cyberattacks, especially in the financial services sector, where the maintenance of highly sensitive NPI creates a particularly attractive and lucrative target for threat actors.

Exposure or Theft of Vast Amounts of Nonpublic Information

Products that use AI typically require the collection and processing of substantial amounts of data, often including NPI.[6] Maintaining NPI in large quantities poses additional risks for Covered Entities that develop or deploy AI because they need to protect substantially more data, and threat actors have a greater incentive to target these entities in an attempt to extract NPI for financial gain or other malicious purposes.

Additionally, some AI requires the storage of biometric data. Biometric data is data derived from an individual's unique physical or physiological characteristics and is often used in authenticator applications. For example, facial and fingerprint recognition are regularly deployed as tools to identify and authenticate an Authorized User.[7] Threat actors can use stolen biometric data to imitate Authorized Users, bypass Multi-Factor Authentication ("MFA"), and gain access to Information Systems that maintain NPI and other sensitive information. They can also use biometric data to generate highly realistic deepfakes.

Increased Vulnerabilities Due to Third-Party, Vendor, and Other Supply Chain Dependencies

Supply chain vulnerabilities represent another critical area of concern for organizations using AI or a product that incorporates AI. AI-powered tools and applications depend heavily on the collection and maintenance of vast amounts of data. The process of gathering that data frequently involves working with vendors and Third-Party Service Providers ("TPSPs").[8] Each

link in this supply chain introduces potential security vulnerabilities that can be exploited by threat actors. As a result, any TPSP, vendor, or supplier, if compromised by a cybersecurity incident, could expose an entity's NPI and become a gateway for broader attacks on that entity's network, as well as all other entities in the supply chain.

Controls and Measures that Mitigate AI-related Threats

The Cybersecurity Regulation requires Covered Entities to assess risks and implement minimum cybersecurity standards designed to mitigate cybersecurity threats relevant to their businesses – including those posed by AI. These cybersecurity measures provide multiple layers of security controls with overlapping protections so that if one control fails, other controls are there to prevent or mitigate the impact of an attack.[9] Below are examples of controls and measures that, especially when used together, help entities to combat AI-related risks.

Risk Assessments and Risk-Based Programs, Policies, Procedures, and Plans

The Cybersecurity Regulation requires Covered Entities to maintain cybersecurity programs, policies, and procedures that are based on cybersecurity Risk Assessments.[10] Such assessments must take into account cybersecurity risks faced by the Covered Entity, including deepfakes and other threats posed by AI, to determine which defensive measures they should implement. Additionally, when designing Risk Assessments, Covered Entities should address AI-related risks in the following areas: the organization's own use of AI, the AI technologies utilized by TPSPs and vendors, and any potential vulnerabilities stemming from AI applications that could pose a risk to the confidentiality, integrity, and availability of the Covered Entity's Information Systems or NPI.[11] The Cybersecurity Regulation requires Risk Assessments to be updated at least annually and whenever a change in the business or technology causes a material change to a Covered Entity's cybersecurity risk to ensure new risks, including those posed by AI, are assessed. Whenever Risk Assessments are updated, Covered Entities should assess whether the identified risks warrant updates to cybersecurity policies and procedures in order to mitigate those risks.[12]

In addition, Covered Entities must establish, maintain, and test plans that contain proactive measures to investigate and mitigate Cybersecurity Events, and to ensure operational resilience, including incident response, business continuity, and disaster recovery plans.[13] The incident response, business continuity, and disaster recovery plans should be reasonably

designed to address all types of Cybersecurity Events and other disruptions, including those relating to AI.

Senior leadership plays a crucial role in prioritizing cybersecurity and establishing a culture that integrates compliance into the entity's overall business strategy. The Cybersecurity Regulation requires the Senior Governing Body to have sufficient understanding of cybersecurity-related matters (including AI-related risks), exercise oversight of cybersecurity risk management, and regularly receive and review management reports about cybersecurity matters (including reports related to AI).[14]

Third-Party Service Provider and Vendor Management

One of the most important requirements for combatting AI-related risks is to maintain TPSP policies and procedures that include guidelines for conducting due diligence before a Covered Entity uses a TPSP that will access its Information Systems and/or NPI.[15] When doing so, DFS strongly recommends Covered Entities consider, among other factors, the threats facing TPSPs from the use of AI and AI-enabled products and services; how those threats, if exploited, could impact the Covered Entity; and how the TPSPs protect themselves from such exploitation.

Covered Entities' TPSP policies and procedures should address the minimum requirements related to access controls, encryption, and guidelines for due diligence and contractual protections for TPSPs with access to Information Systems and/or NPI. In addition, Covered Entities should require TPSPs to provide timely notification of any Cybersecurity Event that directly impacts the Covered Entity's Information Systems or NPI held by the TPSP, including threats related to AI. Moreover, if TPSPs are using AI, Covered Entities should consider incorporating additional representations and warranties related to the secure use of Covered Entities' NPI, including requirements to take advantage of available enhanced privacy, security, and confidentiality options.

Access Controls

Implementing robust access controls is another defensive measure used to combat the threat of deepfakes and other forms of AI-enhanced social engineering attacks, and to prevent threat actors from gaining unauthorized access to a Covered Entity's Information Systems and the NPI maintained on them.[16] One of the most effective access controls is MFA, which the Cybersecurity Regulation requires Covered Entities to implement.[17] As of November 2025, the Cybersecurity Regulation will require MFA to be in place for all Authorized Users attempting to

access Covered Entities' Information Systems or NPI, including customers, employees, contractors, and TPSPs.[18]

MFA requires Authorized Users to authenticate their identities using at least two of three authentication factors: knowledge factors, such as a password; inherence factors, such as biometric characteristics; and possession factors, such as a token.[19] While Covered Entities have the flexibility to decide, based on their Risk Assessments, which authentication factors to use, not all forms of authentication are equally effective. Given the risks identified above, Covered Entities should consider using authentication factors that can withstand AI-manipulated deepfakes and other AI-enhanced attacks by avoiding authentication via SMS text, voice, or video, and using forms of authentication that AI deepfakes cannot impersonate, such as digital-based certificates and physical security keys. Similarly, instead of using a traditional fingerprint or other biometric authentication system, Covered Entities should consider using an authentication factor that employs technology with liveness detection or texture analysis to verify that a print or other biometric factor comes from a live person.[20] Another option is to use authentication via more than one biometric modality at the same time, such as a fingerprint in combination with iris recognition, or fingerprint in combination with user keystrokes and navigational patterns.

In addition to MFA, the Cybersecurity Regulation requires Covered Entities to have other access controls in place that limit the NPI a threat actor can access in case MFA fails to prevent a threat actor from gaining unauthorized access to Information Systems.[21] Covered Entities have flexibility to decide, based on their Risk Assessments, what controls to implement and how to implement them; however, the controls must limit an Authorized User's access privileges to only those necessary for that Authorized User's job functions, and limit the number of Authorized Users with elevated permissions and access to NPI.[22] Covered Entities also must periodically, but at a minimum annually, review access privileges to ensure each Authorized User only has access to NPI the Authorized User needs to perform their job functions and must remove or disable access privileges that are no longer necessary, promptly terminate access privileges following departures, and impose restrictions on how Authorized Users can access devices remotely.[23]

Cybersecurity Training

Another important and required cybersecurity control that can be used to combat AI-related threats is to provide training for all personnel, including senior executives and Senior Governing Body members. The training should ensure all personnel are aware of the risks posed by AI, procedures adopted by the organization to mitigate risks related to AI, and how to respond to

AI-enhanced social engineering attacks.[24] In addition, Covered Entities must provide training specifically designed for cybersecurity personnel.[25] That training should include how threat actors are using AI in social engineering attacks, how AI is being used to facilitate and enhance existing types of cyberattacks, and how AI can be used to improve cybersecurity.[26]

If deploying AI directly, or working with a TPSP that deploys AI, relevant personnel should be trained on how to secure and defend AI systems from cybersecurity attacks, and how to design and develop AI systems securely.[27] Such understanding is essential for developing effective measures that can protect against AI-related threats. If other personnel are permitted to use AI-powered applications, they should be trained on how to draft queries to avoid disclosing NPI.

Although the Cybersecurity Regulation always has required cybersecurity training for all personnel, Covered Entities must now provide at least annual cybersecurity awareness training that includes social engineering.[28] Training on social engineering, including on deepfake attacks, can be effectively delivered through simulated phishing, and voice and video impersonation exercises. Training should cover procedures for what to do when personnel receive unusual requests such as a request for credentials, an urgent money transfer, or access to NPI. For example, trainings should address the need to verify a requestor's identity and the legitimacy of the request if an employee receives an unexpected money transfer request by telephone, video, or email. Moreover, trainings should address circumstances in which human review and oversight must be included in verification procedures.

Monitoring

In order to detect unauthorized access to, use of, or tampering with Information Systems, especially those on which NPI is maintained, Covered Entities must have a monitoring process in place that can identify new security vulnerabilities promptly so remediation can occur quickly.[29] The Cybersecurity Regulation also requires Covered Entities to monitor the activity of Authorized Users as well as email and web traffic to block malicious content and protect against the installation of malicious code on their Information Systems.[30] Covered Entities that use AI-enabled products or services, or allow personnel to use AI applications such as ChatGPT, should also consider monitoring for unusual query behaviors that might indicate an attempt to extract NPI and blocking queries from personnel that might expose NPI to a public AI product or system.

Data Management

Effective data management will limit the NPI at risk of exposure if a threat actor gains access to an entity's Information Systems. Covered Entities are required to implement data minimization

practices as they must dispose of NPI that is no longer necessary for business operations or other legitimate business purposes, which includes NPI used for AI purposes.[31] This practice will decrease the ultimate impact of data breaches as there will be less potential for unauthorized access to, or exfiltration of, NPI. Additionally, although not required until November 1, 2025, Covered Entities should maintain and update data inventories as they are crucial for assessing potential risks and ensuring compliance with data protection regulations.[32] Data inventories further help entities track NPI so that if there is a breach, they know what NPI may have been exposed and what systems were impacted. Entities should implement data governance procedures that include data collection, storage, processing, and disposal.[33]

Moreover, if an entity uses AI or relies on a product that uses AI, controls should be in place to prevent threat actors from accessing the vast amounts of data maintained for the accurate functioning of the AI. In these cases, entities should identify all Information Systems that use or rely on AI, including, if applicable, the Information Systems that maintain, or rely on, AI-enabled products and services. These entities also should maintain an inventory of all such systems and prioritize implementing mitigations for those systems that are critical for ongoing business operations.[34]

Conclusion

While each organization must evaluate and mitigate the risks relevant to their own business, this Guidance highlights some of the current cybersecurity risks associated with AI that all organizations should consider when developing a cybersecurity program and implementing cybersecurity controls. In addition to AI-related risks, organizations should explore the substantial cybersecurity benefits that can be gained by integrating AI into cybersecurity tools, controls, and strategies. AI's ability to analyze vast amounts of data quickly and accurately is tremendously valuable for: automating routine repetitive tasks, such as reviewing security logs and alerts, analyzing behavior, detecting anomalies, and predicting potential security threats; efficiently identifying assets, vulnerabilities, and threats; responding quickly once a threat is detected; and expediting recovery of normal operations.

As AI continues to evolve, so too will AI-related cybersecurity risks. Detection of, and response to, AI threats will require equally sophisticated countermeasures, which is why it is vital for Covered Entities to review and reevaluate their cybersecurity programs and controls at regular intervals, as required by Part 500.

Full Definitions of Part 500 Terms Used

Herein:

Authorized user is defined in 23 NYCRR § 500.1(b) as “any employee, contractor, agent or other person that participates in the business operations of a covered entity and is authorized to access and use any information systems and data of the covered entity”.

Covered entity is defined in 23 NYCRR § 500.1(e) as “any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies.”

Cybersecurity event is defined in 23 NYCRR § 500.1(f) as “any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.”

Cybersecurity incident is defined in 23 NYCRR § 500.1(g) as “a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that:

1. impacts the covered entity and requires the covered entity to notify any government body, self-regulatory agency or any other supervisory body;
2. has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or
3. results in the deployment of ransomware within a material part of the covered entity’s information systems.”

Information system is defined in 23 NYCRR § 500.1(i) as “a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems”.

Nonpublic information is defined in 23 NYCRR § 500.1(k) as “all electronic information that is not publicly available information and is:

1. business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity;
2. any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number; (ii) drivers’ license number or

non-driver identification card number; (iii) account number, credit or debit card number; (iv) any security code, access code or password that would permit access to an individual's financial account; or (v) biometric records;

3. any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to: (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family; (ii) the provision of health care to any individual; or (iii) payment for the provision of health care to any individual."

Risk assessment is defined in 23 NYCRR § 500.1(p) as "the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an Information System. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place."

Senior governing body is defined in 23 NYCRR § 500.1(q) as "the board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer or officers of a covered entity responsible for the covered entity's cybersecurity program. For any cybersecurity program or part of a cybersecurity program adopted from an affiliate under section 500.2(d) of this Part, the senior governing body may be that of the affiliate."

Third-party service provider is defined in 23 NYCRR § 500.1(s) as "a person that:

1. is not an affiliate of the covered entity;
2. is not a governmental entity;
3. provides services to the covered entity; and
4. maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity."

---

[1] New York State defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action. The

definition includes but is not limited to systems that use machine learning, large language model, natural language processing, and computer vision technologies, including generative AI." See https://its.ny.gov/system/files/documents/2024/01/nys-p24-001-acceptable-use-of-artificial-intelligence-technologies-_1.pdf.

[2] Covered Entity is defined in 23 NYCRR § 500.1(e). Capitalized terms used herein are defined in the Cybersecurity Regulation. Section references used herein refer to sections in 23 NYCRR § Part 500.

[3] There has been a 3,000% increase in deepfakes according to Onfido's Identity Fraud Report 2024. https://www.ibm.com/blog/deepfake-detection/.

[4] Information System is defined in § 500.1(i); Nonpublic information is defined in § 500.1(k).

[5] For example, in February 2024, a Hong Kong finance worker was tricked into transferring $25 million to threat actors after they set up a video call in which every other person participating, including the Chief Finance Officer, was a video deepfake. See https://www.bankinfosecurity.com/fraudsters-deepfake-entire-meeting-swindle-255m-a-24273. Other similar examples abound. See, e.g., https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/ (a senior executive at a UK-based energy firm was tricked into wiring €220,000 to the account of a threat actor using an AI-generated voice deepfake that accurately mimicked the distinct German accent and tone of the chief executive of the firm's parent company, who requested the urgent wire transfer of funds); https://www.theregister.com/2022/08/23/binance_deepfake_scam/ (threat actors created a deepfake "AI hologram" of a Binance PR executive that was used to conduct Zoom video calls with companies asking Binance to list their digital asset on Binance.com); https://findbiometrics.com/deepfake-ai-scammers-steal-11m-from-crypto-account/ (threat actor used deepfake technology to bypass facial recognition security measures and drained company's cryptocurrency account of $11 million); https://thehackernews.com/2023/09/retool-falls-victim-to-sms-based.html (threat actors used deepfake voice to trick employee into providing multi-factor authentication code leading to the theft of $15 million in cryptocurrency).

[6] See https://cloud.google.com/learn/what-is-artificial-intelligence ("AI systems learn and improve through exposure to vast amounts of data"), and https://www.ibm.com/blogs/nordic-msp/what-huge-volume-of-data-are-required-for-smart-ai/ (AI algorithms require terabytes or petabytes of data).

[7] Authorized user is defined in 23 NYCRR § 500.1(b).

[8] Third-party service provider is defined in § 500.1(s).

[9] See e.g., principle of "defense-in-depth", https://csrc.nist.gov/glossary/term/defense_in_depth. Defense-in-depth includes robust network segmentation to impede lateral movement across a network. Although not specifically required by Part 500, entities should segregate networks where practicable to enhance security.

[10] See §§ 500.2 and 500.3. Risk Assessment is defined in § 500.1(p). The Risk Assessment should take into account a Covered Entity's size, business model, and complexity as well as the type of data it maintains. Measures and controls implemented should be proportionate to the Covered Entity's resources and risks.

[11] See § 500.11.

[12] See §§ 500.2, 500.3, and 500.9.

[13] See § 500.1(f); See § 500.16(a).

[14] See § 500.4(d); Senior governing body is defined in § 500.1(q).

[15] See § 500.11(a).

[16] See § 500.7.

[17] See § 500.12. As DFS has stated in its *Guidance on Multi-Factor Authentication*, MFA "is one of the most potent ways to reduce cyber risk".

[18] See § 500.12. Notably, MFA has been required by the Cybersecurity Regulation since it was first promulgated in 2017.

[19] See § 500.1(j).

[20] See https://www.bankinfosecurity.com/ai-vs-ai-fighting-deepfakes-biometric-authentication-a-25354.

[21] See § 500.7. While not explicitly required by the Cybersecurity Regulation, best practice is to employ "zero trust" principles, meaning Covered Entities should not implicitly trust the identity of any Authorized User by default. Covered Entities should, to the extent possible and appropriate to their risks, require authentication to verify the identity of an Authorized User each time the Authorized User wants to access an Information System with NPI maintained thereon. See e.g., https://www.nist.gov/publications/zero-trust-architecture.

[22] See § 500.7(1) and (2). For example, someone on the internal audit team should have their normal user account for their daily work (e.g., email access and the ability to log into the user's

workstation) and a privileged account for reviewing information needed to audit that is read-only since there would be no need to make changes.

[23] See § 500.7(a)(4), (5) and (6).

[24] See § 500.14(a)(3).

[25] See § 500.10(a)(2),

[26] Covered Entities may want to consider using a commercial cybersecurity awareness training product that includes AI-related risk content. Some of these offerings incorporate AI to create risk-profiles for the personnel being trained, to create customized phishing simulations and training suggestions based on those personnel's individual knowledge and skill level.

[27] For example, MITRE ATLAS maintains a knowledge base of adversary tactics and techniques based on real-world attack observations and realistic demonstrations from AI red teams and security groups. https://atlas.mitre.org/pdf-files/MITRE_ATLAS_Fact_Sheet.pdf.

[28] See § 500.14(a)(3).

[29] See § 500.5(b).

[30] See §§ 500.5(b) and 500.14(a)(2); 23 NYCRR § 500.14(a)(1) requires Covered Entities to implement risk-based policies, procedures and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, NPI by such Authorized Users.

[31] See § 500.13(b).

[32] See § 500.13(a).

[33] See § 500.3(b).

[34] See § 500.13. As of November 1, 2025, a Covered Entity must maintain these inventories for all of the Covered Entity's Information Systems. Covered Entities with AI assets should consider implementing these asset inventory requirements immediately, at least with respect to their AI assets.

Department of Financial Services

About Us

Mission and Leadership

Advisory Boards

Institutions That We Supervise

Website

Accessibility & Reasonable Accommodations

Disclaimer

Privacy Policy

Site Map

State Laws & Regulations

State Codes, Rules & Regulations (NYCRR)

State Laws (LBDC)

State Bills & Laws (Senate)

Language Assistance

Language Access Policies and Plans

CONNECT WITH US

TWITTER

LINKEDIN

FACEBOOK

REGISTER TO VOTE

Register to vote or update your voter information online.

Translate

Translation Services

This page is available in other languages

- English
- Español
- 中文

- 繁體中文
- Русский
- יידיש
- বাংলা
- 한국어
- Kreyòl Ayisyen
- Italiano
- العربية
- Polski
- Français
- اردو