Liveness Detection: Biometric Frontline or Final Frontier?

facetec

Introduction:
It’s Alive! (Or is it?)

WHY LIVENESS DETECTION IS THE ANSWER TO BIOMETRICS' MOST CRITICAL QUESTION

Although face biometrics have been portrayed in popular media for decades, the technology never reached its full potential outside the silver screen until 2018. No longer relegated to the realms of science fiction, face biometrics have begun to reach their potential to ensure trust and safety. It took revolutions in artificial intelligence (AI) and computer vision to empower face biometrics with enough precision to enhance our lives and protect our privacy, allowing us to finally claim our identity in digital spaces.

Face biometrics are commonly referred to as facial recognition (FR), but it is critically important to understand that what most people call facial recognition is just part of the technology required to realize its potential in the real world. Facial recognition predicts the probability that two different photos contain face data from the same person, essentially forecasting that the individuals are a match. It’s often used by law enforcement to identify a face in a crowd, but when it comes to our account security the correct term is face authentication (FA). Though these two similar concepts are often lumped together by laypeople, the privacy-enhancing application of biometric face authentication technology is not the same as facial recognition used in surveillance or photo sorting. To understand what makes the applications so different, the concept of “liveness detection” must be first understood.

The face is an individual's primary identifier and is the most important and unique part of our physically visible identity. FA does use FR as a part of the process, but with very different intentions. Facial recognition, which scans faces in order to match them with photos in a database of many, puts the inherent power of identity in the hands of others (A key term is “matching”, whereby the sensor matches what it sees with saved images). Law enforcement agencies, governments, marketers working in unregulated markets, and other parties scan individuals to see if they are on watch lists, shoplifter databases or VIP customer lists. It is identification for the enlightenment of the scanning party.

On the other hand, verifying an identity with face authentication empowers the subject user. Biometric FA protects valuables like currency, account numbers, trade secrets, health records, and other confidential information from being wrongfully accessed and can even protect the user from physical harm. Designed for one-to-one matching (not one-to-many, where what a sensor sees is compared against a vast database), face authentication compares the subject user’s face to a single template. If the user matches all of the requirements set forth by the corresponding organization, they will be allowed to proceed. The method is becoming increasingly popular because of the proliferation of premium smartphones, such as the iPhone X, its successors and increasing number of competitors, with specialized hardware allowing for 3D facial recognition. Here, face biometrics bypass a PIN or a password and unlock a device. It’s been promoted as a better access method because it can’t be stolen or forgotten, though in these cases there is always a PIN or password used to reset the device or re-enroll the biometric.

Face Authentication (FA): The privacy-enhancing application of facial biometrics to secure digital and physical assets. Distinct from law enforcement and surveillance uses of face recognition, face authentication compares a user’s face to a single biometric template. If it detects a match, and verifies liveness and three dimensionality, access is granted to the rightful user.

But these systems actually increase the attack surface because there are now two access paths: what you know (PIN or password) and what you are; biometrics and a successful bypass of either one provides access. Because of this, PIN/Pass-failsafe on-device face biometrics are not the ultimate lock.

And if that isn’t bad enough, just as hackers can break through password protected and two-factor security systems, they can also circumvent this kind of face biometric by presenting media that reproduces the user’s biometric data to a system. Hackers, fraudsters and otherwise bad actors trick the technology into believing it is “seeing” the authorized user. This attack vector is called a presentation attack, or a spoof, and it represents the single greatest threat to biometric security.

When biometrics first became mainstream, they weren’t trusted to protect much, which was fine until we wanted to use biometrics for more important things like protecting our assets and using government services. The iPhone’s fingerprint sensor did not need to be un-spoofable because every device was siloed and access was decentralized. Bad actors had to first gain access to the device to even take a crack at spoofing it, and there was little incentive to do so because Touch ID protected mostly photos and texts. Today, the reach of digital identity is deep and complex, and it bears much more weight. The valuable data locked behind our security schemes must now be better protected. Just as one short circuit can blow an entire power grid, even one compromised credential can lead to a massive data breach.

(IMAGE VIA TOM'S GUIDE)

Convenience above security – The current state of hardware-based facial recognition as implemented in Samsung’s new Galaxy S10 is creating a negative buzz.

If we want to realize the full potential of biometrics – true unsupervised user authentication – we need to ensure they are sufficiently robust to threats like those above. They must be able to detect and deny sophisticated presentation attacks by identifying the differences between the one authorized user and any and all facsimiles of their identity. Thankfully, innovative and creative research and development, objectively supported by rigorous third-party standardized testing, is enabling biometric authentication to truly transcend its not-so-secure roots, paving the way for a revolution in how we protect our identities in the digital world. And it all hinges on a simple concept that has been anything but simple to create: liveness detection.

PART ONE

Proving a Negative

LIVENESS DETECTION, YOUR BEST DEFENSE IN A WORLD OF DIGITALLY DISTRIBUTED BIOMETRIC DATA

The challenge of achieving robust liveness detection in biometric authentication is by its very nature ever-evolving. A biometric authentication system's most basic function is to accept a positive and reject a negative. But every fraudster is attempting to present an artifact similar enough to the real user that, as far as the system can tell, is the bonafide authorized user. But the vast majority of real-world sessions are not spoof attempts, and therefore presentation attack detection (PAD) must accept real users without any hassles almost every time, yet prove a negative whenever a fraud attempt is made. This decision must be made instantly and with only the information collected through a small 2D camera lens at a low enough resolution that even the least expensive devices are supported. It's a virtually impossible task, but today the physics of light and lenses can be processed by AI to aid in perfecting the art of spoof detection.

For example, if a fraudster tries to crack a face login system without robust liveness, and they present the camera with a high-definition image of the correct user's face, the security system would be fooled. And that makes sense. The system is looking for a specific face, it sees that face, and grants a positive match: **this face image of the user is recognized <u>as</u> the user**. But we all intuitively understand that this is incorrect, even if the algorithms don't. On the other hand, a system with robust liveness can be presented a high-definition picture (or video, doll or mask) of the authorized user and determine that, even though it is shown an image of the user's face, it is not seeing the legitimate, live user. The system rejects artifacts it has proved to be negative: **this is an <u>image</u> of the user, not the real user**.

While face biometrics are great for illustrating examples of the need for biometric liveness detection, they are far from the only modality wanting for spoof protection. Any biometric system requiring the presentation and matching of a body part or physiological process (literally the meaning of biometry) can be vulnerable to facsimiles. Even new biometric modalities that seem un-spoofable by nature, like behavioral biometrics that measure how a user holds her phone, or systems that authenticate based on gait measurement, will be subject to attacks by specialized neural nets. The human body has myriad unique characteristics, but they can all be reproduced as spoofing artifacts. Fingerprints, irises, palm-prints and voices can all be captured, turned into a spoofing artifacts, and presented to biometric authentication systems for spoof attempts.

People often confuse their desire for anonymity with their right to privacy. But just as our faces are viewed by others every time we leave our homes, our biometric data is also publicly accessible. High definition photography, as well as video and audio technology, are deployed ubiquitously and thanks to the social demands of the digital age, we willfully share our biometric data across business and social media platforms. If no media could ever possibly replicate our biometric data, then liveness detection wouldn't be necessary. But since in reality our photos are included in publicly searchable databases and our fingerprints are left on everything we touch, we need liveness detection. The beauty is that once we have liveness detection, those databases that contain our biometric data are of no consequence as a liability because those artifacts cannot spoof the biometric systems. We want to be recognizable online, but we also deserve the privacy and security biometric authentication with liveness detection can provide.

Liveness Detection: A feature of robust biometric systems, liveness detection (also known as Presentation Attack Detection) is the ability for authentication technology to tell the difference between a real user and a synthetic copy of their biometric data. In face authentication, this is the ability to detect when a high definition picture or realistic 3D model is presented in a request for access, rather than the true user's face.

Liveness detection is our defense against the world of digitally distributed biometric data.

Before robust presentation attack detection was achievable, the first major attempt to mitigate spoofing threats was to layer biometrics with multi-factor authentication (MFA). By combining different layers of on-device security, an authentication system becomes more difficult to break into. The idea is that by adding a password, a physical security token, or additional biometric modalities, it essentially creates so many barriers to entry that, for the most part, the time it takes a random fraudster to hack a random victim is not worth the reward. This may work for a while, but eventually it just invites a black market for the biometric data. For example, databases of face/iris/palm photos, fingerprints and voice recordings could be sold on the dark web to the highest bidder, allowing fraudsters to defeat the biometric portion of any MFA system in which the people in the database are enrolled. So the fact remains that without sufficient liveness detection the biometrics in a MFA system are just as vulnerable as the other factors. If combined with a password, lists from previous breaches, phishing, social engineering, or cooperative user fraud, the hacker would have a significant percentage of successful account breaches. Any system that can't tell the difference between your biometrics and an artifact can and will be bypassed. And if a MFA solution is perceived to be more secure than it actually is, the results can be disastrous for the organization and its users.

With biometric liveness detection, not only can an authentication system withstand presentation attacks, but the multi-factor approach, with its additional user-experience friction, is often rendered unnecessary. There's no need to add a deadbolt to a vault door.

In September, 2017, ISO (International Organization for Standardization) published the Presentation Attack Detection 30107 standard for testing biometric software. Since then, sanctioned PAD tests for biometric authentication solutions have emerged to meet the urgent industry and market demands for performance verification. Chief among these third-party assessments is the **iBeta PAD Test**, a rigorous and unforgiving evaluation of a security solution's ability to withstand the most intense presentation attacks. With three levels of achievement, the iBeta test stands out for holding biometric authentication solutions to high standards, and for its tiered certification, both of which help communicate the most appropriate application of a liveness detection system's performance level and sophistication. A Level-1 graduate of iBeta's test is robust against a wide range of readily available spoof-attempt artifacts and approaches that include high-res photos and video, and masks. Level-2 increases the attack efforts by allowing more time and more sophisticated, 3D-detailed artifacts with life-like attributes. And a Level-3 certified system is robust to expensive and time-consuming custom artifacts, and can be trusted in highest-risk/highest-value financial transactions, confidential record access, and sensitive government applications.

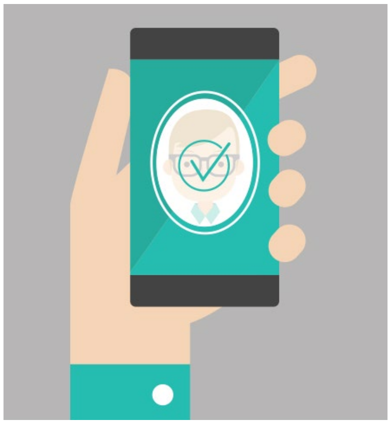
To learn more about the independent PAD testing of biometric authenticators, please see the following white paper:
Anti-Spoof Testing – There's A New Sheriff In Town

PART TWO

The Anatomy of a Spoof

HOW FRAUDSTERS MAKE IT TO FAKE IT

To spoof literally means to "imitate", "hoax", or "trick", and it often carries with it a connotation of humor. In Hollywood, to spoof a topic is to start with something serious and, using its aesthetic properties, create something that subverts the original intention. *Frankenstein*, starring Boris Karloff, is a horror film. But Mel Brooks' spoof of *Frankenstein*, *Young Frankenstein,* is a goofy, vaudevillian romp with all the same characters and symbols, but none of the pathos. This concept can be used to illustrate biometric spoofing, as well. Your physical body is 100-percent real, and you use it to do serious things. A spoofing artifact is not a complete copy of your body's biometric data, but it reproduces enough of your unique traits that "it" can be connected with you, and then used in ways that are anything but funny.



Understand the terms – Fast-moving technology demands clarity, and new ways to accurately describe solutions are constantly emerging. This up-to-date glossary will help you keep pace with the evolution of biometric authentication.

A fraudster might try to spoof a biometric system for the same reasons they will try to crack a password: to gain unlawful access to transfer funds or to personal data which can be sold in online black markets for a profit. Financial data, health care information, and social security numbers are all very valuable, and biometrics are emerging as the best way to protect them. But theft of funds or data are not the only reasons to spoof a system. As we will explore later in this paper, sometimes a spoof is performed with the full knowledge of the true authorized user in his or her absence, perhaps to give a coworker access to a workstation, to enable one student to take a test in place of another in an online class, or to clock-in to a biometric time-and-attendance system.

Regardless of the intention, spoofing methods all share the same common denominator: they rely on a spoofing artifact – a fake fingerprint, a photo, a mask, a voice recording, etc. – to fool a system. Spoofing is not obscure research, and there are quite a few common methods known to successfully break through weaker biometric systems. The wood-glue spoof, for instance, is a simple technique in which a false fingerprint is created using the image of a fingerprint using commonly available carpenter's glue. A replay attack, used to spoof voice biometrics systems, relies on the recording of a user's positive authentication, gained either via malware or more traditional means, allowing a fraudulent user to gain access in their absence. A mask-spoof is exactly what it sounds like: the creation of a mask using a photo of the correct user, and wearing it to trick a face authentication solution.

Far from obscure, you can even use them to test the biometrics systems which you have access to in the comfort of your own home. Many biometric solutions on the market claim to have liveness detection, but really only have simple liveness movement-observation gimmicks. Requiring the user to blink, nod or smile for facial recognition is quite easy to trick. By taking a short video of yourself on your phone and presenting it to a face authentication app on another device, you can turn strong biometric authentication into a simple contactless key system that couldn't be easier to bypass.

When you consider how far other technology industries have come, the fact that such simple spoofs are still susceptible to presentation attack methods is laughable. But it's also concerning, as new advances in artificial intelligence are yielding sophisticated new biometric hacks. Researchers at New York University, for instance, have developed a neural network that can produce so-called **"DeepMasterPrints"** that are capable of tricking one-in-five fingerprints in a given authentication system. **CrazyTalk** software, on the other hand, can be used to create a realistic, 3D, moving virtual avatar of a user's face in a matter of minutes, using a simple profile picture from social media.

It's clear liveness detection gimmicks like smiling, blinking, nodding and moving your head are not enough. If the biometrics industry is going to prove it can solve the digital identity crisis, true innovation is needed.

Spoofing Artifact: A manufactured object intended to fool a biometric system into granting positive authentication. Bad actors are constantly coming up with new and creative spoofing artifacts but common examples include 3D printed masks, voice recordings, and fake fingerprints made of gelatin.

PART THREE

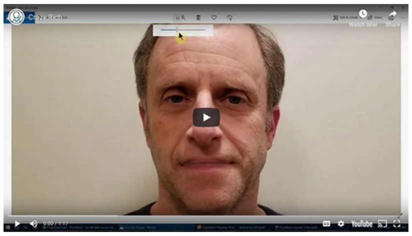
Inside the FaceTec Spoof Lab

WHAT IT TAKES TO PROTECT AGAINST SPOOFING

> **"The FaceTec spoof lab has tens-of-thousands of physical spoof artifacts that we've printed, built or bought over the last five years. We have 3D-printed faces covered in make-up, masks made from user scans, and we've even tested our algorithms at Madame Tussauds Wax Museum. This is the level of commitment that it takes to achieve Level 1&2 certifications."** –Kevin Alan Tussy, CEO, FaceTec

To protect against spoofing, all spoof methods must be understood. Instead of just thinking of biometrics as being inherently secure, think about them as a puzzle. Think: *when this system asks for my face, what is it looking for specifically? Ask: how can I replicate a face using a method the developers didn't consider when building this system?* It takes creativity to be a spoofer, and even more creativity to stop them. This is what drove FaceTec to build such a comprehensive spoof lab.

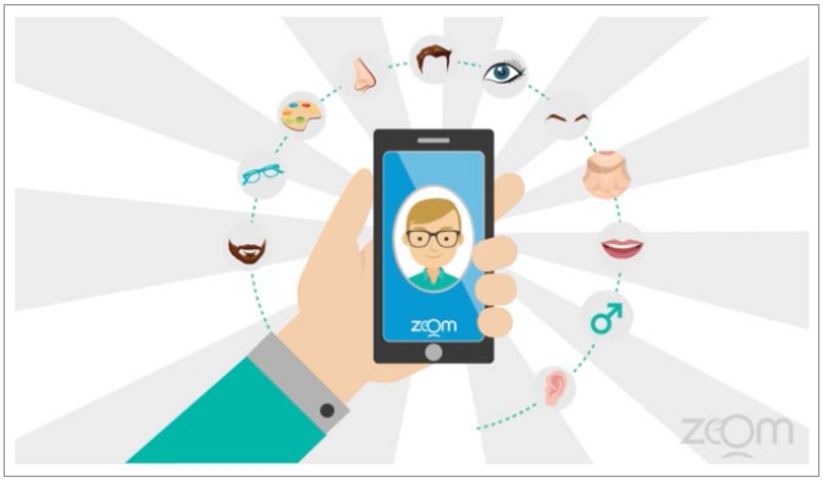
In order to stay a step ahead of the bad guys, preparation is everything. But there must be a "golden balance" in biometrics: they need to provide both security and usability. Recent hardware-focused solutions based on infrared VCSEL technology do a good job of proving user three-dimensionality, but these nascent approaches do not adhere to standardized security levels and use expensive, proprietary components (as with Face ID and its contemporaries), preventing them from ever being deployed as a universal solution.



WATCH: Open sesame – CrazyTalk animation software makes presentation attacks easy. Watch how quickly we can turn a 2D image of FaceTec SVP Business Development Rich Lobovsky into a moving 3D spoof artifact.

ZoOm 3D Face Authentication from FaceTec is a 100% software, platform-agnostic face biometric that works on mobile and desktop devices, and is the first – and only – face authenticator in history to achieve Level 1&2 PAD certifications in sanctioned third-party testing. It is versatile, secure, and accessible enough for users to understand the difference liveness detection can make in real-world use.

“As we continue to reach more users, people will start to see significant differences between what they can do with a fingerprint and what can be done with ZoOm,” said Kevin Alan Tussy, CEO of FaceTec, in an interview with FindBiometrics. “With a fingerprint reader I could check my balance, but with ZoOm I could wire $10,000 without going into a branch, or refinance my mortgage from my couch.”



WATCH: ZoOm combines mind-bending physics and magical AI. The camera lens observes the user’s face warp (via perspective distortion) as it travels through space-time. When AI processes the data, a 3D model of the user’s face is created from a standard 2D camera.

PART FOUR

Teamwork Makes the Dream Work ...OR THE FRAUD

LIVENESS DETECTION DEFENDS AGAINST COMPLICITLY COOPERATIVE USERS

The ultimate goal of presentation attack detection spoof tests is to protect against spoofs involving a cooperative user. A cooperative user is someone enrolled in a biometric authentication system who willfully (though not necessarily knowingly) surrenders their biometric data to a spoofer, essentially handing over the keys to their account.

At first, this scenario seems far-fetched, but consider the scenarios in which passwords and tokens are compromised:

- Away from the office, a user sends credentials to a coworker so they can log into a workstation and retrieve data for good-faith business purposes.
- A part-time employee who is late for work forwards credentials to a work-friend who will sign in on their behalf.
- Malware records the credential without the knowledge of the user.
- A bad actor retrieves credentials via social engineering or phishing.

Cooperative User: A person enrolled in a biometrics system who has their biometric data obtained by a spoofer via willful sharing, social engineering, phishing, or other means. Cooperative users represent the greatest threat to authentication systems and are the benchmark against which Presentation Attack Detection must be tested.

In the movie thriller ***Searching***, a father gains access to his missing daughter's FaceBook, Venmo, messaging, video streaming and bank accounts **by daisy-chaining** simple email password reset procedures together. While in the movie the unapproved access is more than justified, it is easy to see how weak security measures can be abused. Also highlighted is how the lack of digital identity verification in the anonymous online accounts of classmates present a daunting task for investigators.

While these are all known threats to knowledge- and token-based systems, they are equally applicable to biometrics. And even though some cooperative users are sharing credentials for innocuous purposes, such as data retrieval for remote work, the reality is that an impersonation can occur. The viable spoof artifact has created a dire vulnerability for the enterprise in need of liveness detection. Two of the largest data breaches of the past five years, affecting Uber and TimeHop users, were committed using only one set of compromised credentials.

Recent articles have alerted us to the possibility that Know Your Customer (KYC) data has **already been breached** and is for sale on the Dark Web. With dozens of companies now collecting KYC data, which includes a **selfie and photos** of identification documents such as driver's licenses and passports, it's only a matter of time until all of our digitized identity info is breached and password-stuffing will give way to KYC data-stuffing.

These articles highlight the need for robust, certified 3D liveness, as any system without it would be instantly vulnerable to new account fraud using these selfies. With 3D liveness detection in place, the challenge to any fraudster is exponentially more difficult. With ZoOm, it is practically impossible: the spoofer would have to transform the digital 2D data into an accurately rendered recreation of a living 3D person.

“With **CrazyTalk animation software** you can do that well enough to spoof most "authenticators" in the market, but not ZoOm,” said Josh Rose, FaceTec CTO. “When the fraudster tries to use a selfie to spoof ZoOm, no matter what they try – avatars, photoshop filters to simulate face bending, printing and glueing to a 3D mask, etc. – it still won't fool ZoOm’s liveness detection. This is because ZoOm also detects generation loss (a reduction in the quality of a representation of an original image); like when a photocopier makes a copy of a copy and the small details are lost.”

Imposter access is the most glaring vulnerability in information security, and targeted biometric data is the most likely attack vector from spoofers. A cooperative user test is a proper benchmark requirement for liveness detection because it accurately simulates breaches where the spoofer has access to the type of biometric data needed to target a victim.

Fraud is a business, and it’s a numbers game. Bad actors will always look for the path of least resistance to gaining access to valuable data, and just as with passwords, the quickest way to get the biometric key is to have it given to you.

PART FIVE

Adopt High Standards or Become Low-Hanging Fruit

THE STAKES ARE HIGH, LIVENESS DETECTION IS NOT NEGOTIABLE

Emerging testing standards like the **ISO-guided iBeta NIST/NVLAP-certified PAD test** are critically important because they bring transparency, accountability and honesty to vendors' biometric performance claims. In its scramble to meet skyrocketing demand, and in the absence of liveness detection breakthroughs, the industry itself has taken to marketing hype and false claims of security. Rigorous to the point of controversy, firms like iBeta can now provide a full understanding of – and trust in – the abstract idea that liveness detection in biometric authentication technology can provide effective protection against the most creative spoof attacks imaginable, while allowing easy, day-to-day account access.

No one knows biometrics like the industry itself, and it is the responsibility of vendors, researchers and developers to rise to the challenges set by sanctioned third parties. A high bar is necessary because biometrics may be our last chance at protecting our most sensitive data. If not, the public may lose confidence in our increasingly important digital spaces, with money, personal data, privacy and more on the line for end users, organizations and vendors alike. While the playing field may be virtual, the assets and the consequences are real.

According to **a recent report from Experian**, 2019 will be the year biometrics systems are truly tested in the wild by bad actors. Thanks to their ubiquity and increasing value, biometric authentication solutions are now guarding the assets that have put them in the crosshairs of fraudsters and hackers. Unlike third-party standards assessments, the real-world biometric security fails will cause real pain to real people. We are approaching the last chance for biometrics to prove they're ready for the sober job of authentication.

High standards can be held by fostering healthy competition and transparent practices. Leading by example, FaceTec has been fighting data breaches on the front lines by protecting users with truly robust, certified authentication technology that understands the difference between a human being and a spoof. Certified liveness detection ensures that only the original key opens the door, copies of the key won't work.

Conclusion: Staying Alive

BIOMETRICS WILL SURVIVE THANKS TO 3RD-PARTY-CERTIFIED LIVENESS DETECTION

Standardized biometric PAD testing promises to boost the biometric authentication industry to new heights, making good on its potential of true convenience and real security. Thanks to iBeta's PAD tests, biometrics vendors can rise to the occasion and provide users with robust authentication solutions that can prevail over the next generation of inanimate security threats. Complicit users, phishing and even black-hat AI stand ready to end the biometric revolution before it starts. But if the biometrics industry sets its standards high, then it will survive.

To learn more about the rigorous standardized biometric PAD testing offered by iBeta, along with an in-depth investigation into the rise of standards, read our first white paper in this series: **Standardized Testing for Biometrics – Cutting through the hype and finding integrity in digital identity.**

About FaceTec

FaceTec provides class-leading biometric authentication solutions for mobile and web applications requiring certified, high-performance liveness detection. Leveraging decades of computer vision, artificial intelligence and advanced biometrics experience, FaceTec developed ZoOm, the iBeta PAD Level-1 and Level-2 Certified 3D face authentication platform for iOS, Android, mobile and desktop browsers/webcams. The only unphishable and unshareable biometric modality, ZoOm is ideal for onboarding and virtually any identity and access management requirement.

Founded in 2013 with offices in San Diego, CA; NY, NY; London, UK; and Summerlin, NV, FaceTec provides biometric security on five continents for organizations in financial services, mobile payments, border security, connected transportation, digital identity and onboarding, and more. For more information and business inquiries, please visit www.ZoOmLogin.com.