Because no two automated-driving technologies are exactly alike, SAE International’s standard J3016 defines six levels of automation for automakers, suppliers, and policymakers to use to classify a system’s sophistication. The pivotal change occurs between Levels 2 and 3, when responsibility for monitoring the driving environment shifts from the driver to the system.

**Level 0 _ No Automation**

*System capability:* None. • *Driver involvement:* The human at the wheel steers, brakes, accelerates, and negotiates traffic. • *Examples:* A 1967 Porsche 911, a 2018 Kia Rio.

**Level 1 _ Driver Assistance**

*System capability:* Under certain conditions, the car controls either the steering or the vehicle speed, but not both simultaneously. • *Driver involvement:* The driver performs all other aspects of driving and has full responsibility for monitoring the road and taking over if the assistance system fails to act appropriately. • *Example:* Adaptive cruise control.

**Level 2 _ Partial Automation**
System capability: The car can steer, accelerate, and brake in certain circumstances. • Driver involvement: Tactical maneuvers such as responding to traffic signals or changing lanes largely fall to the driver, as does scanning for hazards. The driver may have to keep a hand on the wheel as a proxy for paying attention. • Examples: Audi Traffic Jam Assist, Cadillac Super Cruise, Mercedes-Benz Driver Assistance Systems, Tesla Autopilot, Volvo Pilot Assist.

Level 3 _ Conditional Automation

System capability: In the right conditions, the car can manage most aspects of driving, including monitoring the environment. The system prompts the driver to intervene when it encounters a scenario it can’t navigate. • Driver involvement: The driver must be available to take over at any time. • Example: Audi Traffic Jam Pilot.

Level 4 _ High Automation

System capability: The car can operate without human input or oversight but only under select conditions defined by factors such as road type or geographic area. • Driver involvement: In a shared car restricted to a defined area, there may not be any. But in a privately owned Level 4 car, the driver might manage all driving duties on surface streets then become a passenger as the car enters a highway. • Example: Google’s now-defunct Firefly pod-car prototype, which had neither pedals nor a steering wheel and was restricted to a top speed of 25 mph.

Level 5 _ Full Automation

System capability: The driverless car can operate on any road and in any conditions a human driver could negotiate. • Driver involvement: Entering a destination. • Example: None yet, but Waymo—formerly Google’s driverless-car project—is now using a fleet of 600 Chrysler Pacifica hybrids to develop its Level 5 tech for production.

Auto•No•Mo’•Us: Return to Full Coverage

Find a Vehicle Near You

Enter your ZIP Code to discover local offers on new and used vehicles.

94940

Shop Local Cars
This Is the Tech Fully Autonomous (Level 5) Cars Will Need To Have

Of all the challenges in putting a robocar on the road, figuring out the hardware may be the easy part.

A Level 5 vehicle—a steering-wheel-less car in which the passenger is never a driver—needn’t look like a koala-faced kid’s toy with a chicken bucket fixed atop its roof. Supplier Continental, a key player in the technology involved in automated driving, imagines its compact and flush-mounted sensors can be adapted to fit the familiar shapes and styles of current cars. Can full automation be achieved with fewer sensors, such as Tesla’s proposal to rely on a handful of cameras? “That’s a tricky question,” says Ibro Muharemovic, Continental’s head of advanced engineering. Yes, one system could accomplish the task. For safety purposes, however, he says redundancy is key. Every system must have a fail-safe backup. Here’s a look at the equipment Continental envisions enabling the highest level of automated driving:

Lidar

High-resolution lidar (light detection and ranging) sensors will map surrounding objects up to three football fields away with five-nanosecond bursts of laser that bounce back to the sensors, even through inclement weather or the dark of night. The compact sensors, which capture images of the
environment in 30 milliseconds, have no moving parts, making them more durable and easier to discreetly integrate into a vehicle.

- **Ultrasonic sensors**

Eight quarter-sized proximity sensors measure the distance between the vehicle and surrounding objects in low-speed situations and also provide cross-traffic information.

- **Radar**

Already widely used for adaptive cruise control, radar sensors will be updated, changing from square to a more curved shape when applied to a car’s corners, providing a wider field of view. Front radar units can look up to 900 feet ahead while rear sensors can see as far as 1800 feet to identify fast-approaching traffic.

- **High-definition mapping**

Cross-referencing the information coming from the car’s cameras and radar and lidar sensors with a high-definition map stored onboard will place the car in its environment with a huge degree of accuracy. Mapping companies, such as Here and TomTom, are capable of pinpointing objects down to the centimeter.

- **Cameras**

Cameras—particularly depth-perceiving stereo cameras—mimic the human eye to monitor changing conditions, though they never blink or get distracted by a squirrel. That said, their daylight range is limited to roughly 300 feet compared with a human’s 3000-foot visual acuity, so that will have to improve. Cameras also can provide a 360-degree surround view for parking.

- **Backup brake actuator**

In case of a primary system failure, an emergency electronically controlled actuator will apply pressure to the hydraulic system to slow the vehicle.
**Tire monitors**

Continental’s electronic tire-monitoring system, eTIS, mounts a sensor inside the tire rather than on the valve stem. This allows more accurate readings of tire temperature, load, balance, and even tread condition—information that will help the computer determine when it needs to increase following distances to leave more space for emergency braking.

**V2X communications**

Dedicated short-range radio frequencies can transmit live data more than 3000 feet from one vehicle to another (V2V) or to devices carried by pedestrians (V2P). Doubling down, information will also pass from vehicle to cloud and down to other vehicles via cellular networks (V2X), although nascent 5G technology, faster and with greater bandwidth than 4G, may be required to manage the data load.

**Power supply**

To hedge against an electrical failure, two distinct 12-volt circuits will power the system.

**The brains**

Continental’s Assisted & Automated Drive Control Unit translates the many data streams into a real-time 360-degree digital re-creation of the vehicle’s environment. The ADCU will then determine a safe path of travel and course of action, communicating that plan with the vehicle’s drive, steering, and braking systems. Computing capability will vary depending on the visual requirements and redundancies of the systems, ranging from the power of a modern smartphone to that of six quad-core processors.

**Information autobahn**

Already in use for high-definition camera systems, Category 5 ethernet cables will quickly move data received from the sensors to the car’s brains.
The success of AVs will depend on sensible regulation

Smart regulation and smart technology must go hand in hand

REGULATING A COMPLEX new technology is hard, particularly if it is evolving rapidly. With autonomous vehicles just around the corner, what can policymakers do to ensure that they arrive safely and smoothly and deliver on their promise?

The immediate goal is to make sure that AVs are safe without inhibiting innovation. In America, experimental AVs are allowed on the roads in many states as long as the companies operating them accept legal liability. Chris Urmson of Aurora says American regulators have got things right, working closely with AV firms and
issuing guidelines rather than strict rules that might hamstring the industry. “It's important that we don't leap to regulation before we actually have something to regulate,” he says.

At the other end of the spectrum, Singapore’s government has taken the most hands-on approach to preparing for AVs, says Karl Iagnemma of nuTonomy, an AV startup that has tested vehicles in the city-state. For example, it has introduced a “driving test” that AVs must pass before they can go on the road. This does not guarantee safety but sets a minimum standard. The city of Boston has done something similar, requiring AVs to be tested in a small region before roaming more widely.

Elsewhere, regulators have permitted limited testing on public roads but want to see more evidence that the vehicles are safe before going further, says Takao Asami of the Renault-Nissan-Mitsubishi alliance. “Simple accumulation of mileage will never prove that the vehicle is safe,” he says. Instead, regulators are talking to carmakers and technology firms to develop new safety standards. Marten Levenstam, head of product strategy at Volvo, likens the process to that of developing a new drug. First you show in the laboratory that it might work; then you run clinical trials in which you carefully test its safety and efficacy in real patients; and if they are successful, you ask for regulatory approval to make the drug generally available. On this analogy, autonomous cars are currently at the clinical-trial stage, without final approval as yet.

What form would that approval take? Eventually, it will mean formal certification of vehicles capable of operating fully autonomously, so they can be offered for sale. But initial approval is likely to be granted to operators of specific robotaxi fleets, rather than vendors of particular vehicles, suggests Mr Levenstam, because fleet operators will monitor all vehicles closely to ensure and maintain safety. Even this will be a calculated risk. It is not possible to prove that a new drug is entirely safe, but the risk is worth taking because of the benefits the drug provides. It will be the same for AVs, he suggests. After all, the status quo of human-driven vehicles is hardly risk-free.

Mr Asami draws another analogy, with aviation. “Black box” data recorders and careful testing have enabled air transport to evolve, despite crashes, because
passengers know safety is taken seriously. In fact, America’s National Transportation Safety Board (NTSB) has started applying its aviation expertise to autonomous vehicles. In many ways AVs are more complex than aircraft, says Deborah Bruce of the NTSB, because they are closely surrounded by other things that move in unpredictable ways.

But medicine and aviation have global (or at least regional) regulatory standards, whereas AVs do not. The current patchwork of regulation will have to be simplified if the technology is to be widely deployed. “Uniformity is the friend of scalability,” says Mr Iagnemma. Questions of insurance and liability will also have to be worked out. Amnon Shashua of Mobileye worries that because of today’s regulatory uncertainty, fatal accidents involving fully autonomous vehicles could plunge the industry into legal limbo, or kill it altogether. He has proposed a set of rules that define how a car should respond in all 37 scenarios in the 6m-entry accident database maintained by NHTSA, America’s car-safety regulator, and would like to see these rules adopted as an open industry standard. That would absolve carmakers from making implicit ethical choices in their software while leaving room for innovation in other areas. Mr Iagnemma thinks it is a good start. Without such standards, he says, every company will develop its own way of translating the rules of the road, devised for humans, into a code that can be followed by machines.

Political potholes ahead
The risk of a backlash seems real enough. A survey by Advocates for Highway and Auto Safety, a consumer lobby, found that 64% of Americans were worried about sharing the road with AVs. In another survey, by the Pew Research Centre, 56% of Americans said they would not ride in a self-driving vehicle (see chart). Seeing AVs in action will be an important element of building public trust. In cities where AVs are commonplace, drivers have got used to them. Uber, Waymo and others are also starting to provide robotaxi rides in limited areas, so people can discover that
riding in an AV is thrilling for the first 30 seconds and then quickly becomes boring. “But that’s the response we really want,” says Noah Zych of Uber, because it means riders feel safe.

Assuming that AVs can be shown to be safe, regulators will face a second challenge: setting the rules around how and where they operate, and how they relate to other forms of transport. Fine-tuning of pricing will, in theory, let planners control congestion and promote equal access to mobility.

Governments wishing to encourage the adoption of robotaxi services could go further, restricting the use of private cars (Gothenburg, London, Milan, Singapore and Stockholm already have congestion charges of various kinds) or banning them from some areas. That might be unpopular, and not just with car-owners. “I think there will be some real resistance to measures that compel people to use autonomous vehicles,” says Peter Norton of the University of Virginia. AVs could be seen as an Orwellian technology, an instrument of surveillance and social control.

Protesters might object by standing in front of AVs and blocking traffic. That could lead to calls for AV lanes to be fenced off, “thus making city streets even more inhospitable to non-motorists than they already are”, says Brian Ladd, author of “Autophobia”, a history of opposition to cars. But an unregulated introduction of robotaxis could also cause problems. Rival fleet operators might flood the roads with vehicles offering cut-price rides, making congestion worse.

Choices about transport and pricing are inescapably political in nature. How cities deal with them will depend on both economics and political dynamics, notes Justin Erlich of Uber. “We should be exploring lots of different policies in lots of different cities,” he says. Meanwhile, two principles can help.

The first is to consider AVs in the context of the wider transport system, and be clear about what role they are expected to play. AVs might be deployed as the primary means of transport in a particular area; or they could be used in “first mile, last mile” mode to ferry people to and from railway stations, filling mobility gaps and complementing other forms of transport.
The second principle is to **be mindful of the balance of freedoms**. AVs can potentially free people from driving, congestion, pollution and parking—but in return may require them to give up some other freedoms, such as the ability to take their own vehicle anywhere. In liberal countries, AVs will be accepted only if people feel that they enhance freedom rather than reduce it.

A century ago cars raised fundamental questions about personal autonomy, freedom of choice and mobility. AVs will do the same again. But this time around, with the benefit of hindsight, there is a chance that they will be seen not simply as a new form of transport but as a technology with far-reaching social and economic implications. Driverless cars present an opportunity to forge a new and better trade-off between personal mobility and societal impact. But AVs will deliver on their promise only if policymakers—like passengers climbing into a robotaxi—are absolutely clear about where they want to end up.

*This article appeared in the Special report section of the print edition under the headline "Rules of the road"*

---

**Special report: Reinventing wheels**

**More in this special report:**

**Reinventing wheels:**
Autonomous vehicles are just around the corner

**From here to autonomy:**
Autonomous-vehicle technology is advancing ever faster

**Selling rides, not cars:**
Self-driving cars will require new business models

**The new autopia:**
A chance to transform urban planning

**A different world:**
Self-driving cars will profoundly change the way people live

**Rules of the road:**
The success of AVs will depend on sensible regulation
We have a few words for you

If you don’t know the terminology, blockchain can seem either baffling or boring. Here’s a guide to help you make sense of it all.

Alt-coin / A cryptocurrency that works similarly to Bitcoin but with modifications such as being able to process transactions faster.

Blockchain / A structure for storing data in which groups of valid transactions, called blocks, form a chronological chain, with each block cryptographically linked to the previous one.

Consensus protocol / A process, encoded in software, by which computers in a network, called nodes, reach an agreement about a set of data.

Cryptocurrency (or crypto-token) / A scarce digital asset defined by a blockchain protocol and exchanged via that blockchain system.

Decentralization / A hard-to-quantify measure of a network’s resistance to attack, a function of how broadly control is distributed among different actors.

Distributed ledger technology (DLT) / A system, most commonly a blockchain, for creating a shared, cryptographically secured database.

Fork / A change to the way a blockchain’s software rules define valid transactions, or blocks. / Hard fork: A change to the rules that all nodes on a network must adopt, or else leave the network. / Soft fork: A backwards-compatible change that hinges only on a majority of nodes’ adopting the new rules.

Hash function / A cryptography tool that turns any input into a string of characters that serves as a virtually unforgeable digital fingerprint of the data, called a hash.

Initial coin offering (ICO) / A blockchain-based fund-raising mechanism in which entrepreneurs mint new crypto-tokens and sell them to investors.

Mining / The process by which nodes in Bitcoin, Ethereum, and many other blockchain systems (those that use the consensus protocol known as proof of work) add new blocks to their respective chains and generate new crypto-tokens.

Permissioned blockchain / A shared database with a blockchain structure that requires participants to obtain permission before reading or writing to the chain. Contrast this with permissionless blockchains, which anyone can join.

Proof of stake / A novel consensus protocol in which, instead of mining, nodes can validate and make changes to the blockchain on the basis of their existing economic stake.

Proof of work / The consensus protocol of choice for Bitcoin and many other cryptocurrencies. To add a new block, miners must calculate a hash for it that meets certain narrow criteria. Doing so requires an enormous number of random guesses, making it a costly process that deters attempts to commit fraud.

Smart contract / A computer program stored in a blockchain that automatically moves digital assets between accounts if conditions encoded in the program are met. It serves as a way to create a mathematically guaranteed promise between two parties.
A new way to work

What will business technology look like tomorrow?

Two experts from MIT analyse the business implications of our digital future

IN 2014 Andrew McAfee and Erik Brynjolfsson of the Massachusetts Institute of Technology published “The Second Machine Age”. The book was a balanced portrait of how new digital technologies were poised to improve society, even as they increased unemployment and depressed wages. In their latest work, “Machine, Platform, Crowd”, the authors seek to explain the business implications behind these developments.

Mr McAfee and Mr Brynjolfsson believe that the latest phase of computers and the internet have created three shifts in how work happens. The first is artificial intelligence (AI): a move from man to machine. In the past people worked with computers and, at the same time, were augmented by them: what the authors call the “standard partnership”. But that model is breaking down as computers improve and take more control.

You need only look at self-driving cars, online language translation and Amazon’s prototype cashierless shops to see that something big is happening. Digital technologies used to be applied to information—first numbers and text, and, later, music and video. Now, the digital technologies are invading the physical world.
For instance, designing a “heat exchanger”, a part in appliances like refrigerators, means balancing many different specifications and constraints. Humans settle for one that works well enough because to find the optimal one is too hard. But new “generative design” means AI-infused software can run zillions of tiny permutations to find the best possible design—one that a human might not come up with. And with 3D printing, those designs might be shared, modified and manufactured anywhere.

The second is a shift from products to platforms. Many people encounter evidence of this every day. The largest cab service owns no vehicles (Uber), the biggest hotelier has no property (Airbnb), the most comprehensive retailer holds no inventory (Alibaba) and the most valuable “media” company creates some content but not much (Facebook). There are more than 2.2m apps in Apple’s store, almost none of which the company developed itself.

Platforms are a way for companies to create marketplaces that allow both sides of the transaction to flourish—while the firm, as gatekeeper, enjoys a tidy revenue stream. This is hard to pull off. The platform must ensure that standards are high, and also attract different sets of participants (like drivers or app developers on one side and customers on the other). But platforms are very valuable when they work, since they scale beautifully in a digital setting. The meatiest part of the book is the treatment of platform economics, replete with demand-curve charts.

The third shift is from the core to the crowd. The core refers to centralised institutions, like central banks or the “Encyclopedia Britannica”; the crowd refers to the decentralised, self-organising participants, be it bitcoin nodes that manage the virtual currency or contributors to Wikipedia.
When transaction costs are high, companies do things internally, as Ronald Coase, an economist, once noted. Yet as digital technologies lower the cost of interacting, more things can be done by informal groups. This leads to greater experimentation and innovation. “The core is often mismatched for the kinds of challenges and opportunities it faces, while the crowd, because it’s so big, almost never is,” the authors write.

Pedants will quibble that the book is built on individual themes that others have looked at more deeply. Some readers will be aghast that chapters end with bullet-point summaries and questions, evoking the worst of unctuous business tomes. But tolerate this. For an astute romp through important digital trends, “Machine, Platform, Crowd” is hard to beat.

*This article appeared in the Books and arts section of the print edition under the headline "A new way to work"*
Common Fraud Schemes

Fraudsters are constantly inventing new ways to trick people into disclosing personal information and compromising their online security. Staying informed about the common fraud schemes is the first step to identifying malicious activity to help ensure you do not become a victim.

Identity Theft

Identity theft occurs when fraudsters obtain personal information to commit fraud. There are many ways in which a fraudster may collect personal information, which can include obtaining from mail or trash, installing malware on a victim’s device, hijacking personal accounts (e.g., email or social media accounts) and more.

Charity Fraud

Charity fraud is when a fraudster poses as a fake organization, usually during popular times of the year like holidays, awareness months, and political elections.

How to Avoid Falling Victim to Charity Fraud

Always ask for detailed information about the charity and do your research to confirm that it is a legitimate organization.

Elder Abuse

Elder abuse is when fraudsters exploit certain vulnerabilities (e.g., cognitive impairment, lack of familiarity with technology) in the elderly to collect their personal and financial information for economic gains.

Social Engineering Schemes

One of the most common methods fraudsters may use is what is known as social engineering, which involves using false pretenses or misrepresentations to manipulate victims into sharing information. The information may be seemingly innocuous but could later be used to carry out further attacks including identity.

Email Account Takeover

An email account takeover occurs when a fraudster compromises your personal email account and searches your email history or looks for conversations between you and personnel at your financial institution. They will then imitate your former communications to appear legitimate, and finally may send a request to transfer funds (normally via wire transfer) to an external account where the fraudster can access the funds.

How to Avoid Falling Victim to Email Account Takeover

Think before you click on any links or open any attachments. Email compromises are often the result of malware being installed on devices after unknown links are clicked.

Fabricated Online Applications

Fabricated online applications occur when a fraudster creates counterfeit online applications through fake sites that prompt someone to enter login credentials and other personal information.

How to Avoid Falling Victim to Fabricated Online Applications

Check to be sure the web address in your browser starts with https:// (the s stands for ‘secure’). Look for a closed padlock in your web browser. When you click on the padlock you should see a message that states the name of the company and that “The connection to the server is encrypted”.

How to Avoid Falling Victim to Elder Abuse

Educate yourself and your elderly family members/friends on how to monitor accounts and report suspicious activity.
PHISHING messages are communications, which sometimes include a generic greeting requesting your immediate attention to a serious financial problem. Often, these communications will carry an unusually strong sense of urgency to panic the recipient, and the attachments in a phishing email contain malicious software (“malware”). The malware may be ransomware that accesses a victim’s files, locks and encrypts them and then demands the victim to pay a ransom.

Users can also become infected with malware in other ways, such as clicking on unverified links in text messages, social media messages and websites.

HOW TO AVOID FALLING VICTIM TO PHISHING
• Be wary of communications with a strong sense of urgency and unexplained/unexpected emails requesting your personal information.
• Look for misspellings, grammatical errors and incorrect usage of terms.
• Do not click on unknown links, requests or attachments embedded in emails or texts.
• If you are asked to provide personal information via email, contact the company directly by phone using a phone number obtained from a different source to verify.

VISHING attempts are conducted via telephone where fraudsters pose as representatives from legitimate organizations to obtain personal or financial information. Similar to phishing, these calls have a sense of urgency that will create a sense of panic making you more likely to share the requested personal information.

HOW TO AVOID FALLING VICTIM TO VISHING
• Do not share your information over the phone unless you have initiated the request.
• When receiving an unexpected call, hang up and contact the organization using the contact details that are on your account statements, your credit card or the institution’s official webpage.

SMiSHING is similar to phishing and vishing in the way that it uses elements of social engineering to trick you into visiting a malicious website or providing private information. SMiSHing is conducted via text or SMS, but can also occur through other messaging apps, such as WhatsApp.

HOW TO AVOID FALLING VICTIM TO SMiSHING
• When receiving a text message that contains a link, always verify with the sender before clicking on the link. Messages received from an unknown number, refrain from responding or clicking on the link.
• Do not share private information on any unknown or unverified website or in response to texts from unknown senders.

COMPUTER TECHNICIAN SCHEME
A fraudster will pose as an IT representative from a software company, with the objective of persuading you to grant them remote access to your device(s). Typically, these fraudsters will call you, alerting you of a “critical” or “serious” system issue that requires immediate remediation.

HOW TO AVOID FALLING VICTIM TO A COMPUTER TECHNICIAN SCHEME
• Do not give out personal, computer and/or account information to a third party via email or incoming phone call.
• Request identification (e.g., employee ID, department, etc.) from the caller and obtain a callback number.
• If you have a device that is malfunctioning, call the legitimate vendor for assistance with your inquiries at the number provided at the time of purchase.
FAMILIAL SCHEME
In this scheme, a fraudster will pretend to be a family member or friend in trouble, requiring immediate financial assistance to avoid “serious consequences.” This scam can happen through a phone call, email or social media, and it takes advantage of the relationship between you and a loved one to facilitate the quick transfer of money with minimal questions asked.

HOW TO AVOID FALLING VICTIM TO A FAMILIAL SCHEME
Reach out to known family members or friends, via legitimate contact numbers and/or communication methods, to confirm their circumstances before providing any monetary assistance to the caller.

ROMANCE SCHEME
A fraudster will usually use social media applications or dating websites to initiate communications and build rapport. These scams are typically characterized by a need to communicate privately (e.g., via email, phone, etc.) to strengthen the relationship. The stories are designed to elicit emotional responses and make you more agreeable to send aid.

HOW TO AVOID FALLING VICTIM TO A ROMANCE SCHEME
• Do not disclose personal, computer and/or account information to people you meet online.
• Do not send money to anyone you do not know or with whom you do not have a relationship, including people you meet online.

ADVANCED FEE AND LOTTERY SCHEME
The fraudster will attempt to persuade you to pay money upfront or “a fee” in anticipation of receiving something of greater value in return. This fee may be marketed as a commission, taxes or regulatory in nature.

HOW TO AVOID FALLING VICTIM TO ADVANCE FEE AND LOTTERY SCHEME
Fraudsters can execute this scheme in a number of different ways, each with its own banking vehicle and reward type; therefore, be wary of requests for upfront costs in return for value or a reward. Legitimate corporations would not ask you to pay an upfront cost for an unsolicited reward.

How Clients Can Protect Themselves

While Morgan Stanley takes great care to secure your assets and your information, you and your family also play an important role in defending against fraudulent activity to prevent you from falling prey to cyberattacks. Cyberattacks are increasing in volume and frequency, and cybercriminals are getting more creative.

PII normally includes:

GOVERNMENT-ISSUED PERSONAL IDENTIFIER National ID number (i.e., Social Security number), tax ID number, passport number, diver’s license number, state ID number, etc.

ACCOUNT INFORMATION Account number, debit card/credit card number, username, PIN/password, etc.

CONTACT DETAILS Email address, phone numbers, mailing address.

You can help prevent yourself from becoming a victim of identity theft by protecting your PII. Be wary of whom you share information with. To learn about how to keep yourself and your family safe and more secure online, visit the Department of Homeland Security website at www.dhs.gov/stopthinkconnect. On the next page are some quick tips on how to safeguard your information.
Top Ways to Boost Your Cybersecurity

**CHOOSE STRONG PASSWORDS.** Change your passwords frequently and keep them confidential. A robust password strategy is your first line of defense against hackers. Your passwords should be unique and include a combination of uppercase and lowercase letters, numbers and special characters. Also, avoid reusing passwords across multiple sites.

**AVOID USING PUBLIC WI-FI.** Avoid accessing personal information or entering your password on a site or mobile application over public Wi-Fi connections, as public networks are often not secure. Instead, create a personal Wi-Fi hotspot with your phone and use it to log in to sensitive sites.

**INSTALL THE LATEST ANTI-VIRUS SOFTWARE.** The latest anti-virus software helps keep you safe by detecting the most current and active viruses that could infiltrate your computer to obtain your personal data and information.

**ACTIVATE MULTI-FACTOR AUTHENTICATION.** As a Morgan Stanley client, you can enable an additional factor of authentication in addition to your username and password on Morgan Stanley Online and the Morgan Stanley Mobile App. Log in to your account and visit the Services tab, Profile + Settings, Login Security Preferences to learn more.

**ENROLL IN ACCOUNT ALERTS AND NOTIFICATIONS.** Enrolling in alerts and notifications for your account, allows you to better manage your account and helps you detect suspicious or unfamiliar activity almost as soon as it happens.

**SHRED ACCOUNT DOCUMENTS.** Tax records and other sensitive documents before disposal.

**USE THE LATEST OPERATING SYSTEMS AND SOFTWARE.** It is important to make sure your web browser and operating systems are up-to-date.

**BE CAREFUL OF WHAT YOU POST ON SOCIAL MEDIA.** When using social media be careful about sharing personal information such as your birth date, birthplace, passwords, Social Security number, phone numbers, credit card numbers, bank account numbers and other financial information. Details like these could be used to try and guess passwords or additional security questions.

**MONITOR YOUR CREDIT.** Even the most vigilant individual can still fall prey to cyberattacks that result in fraud. That’s why it’s always a good idea to keep tabs on your accounts to look for signs of identity theft or unauthorized purchases.