Securing your home

Living in a digital environment means being aware of cybersecurity at home.

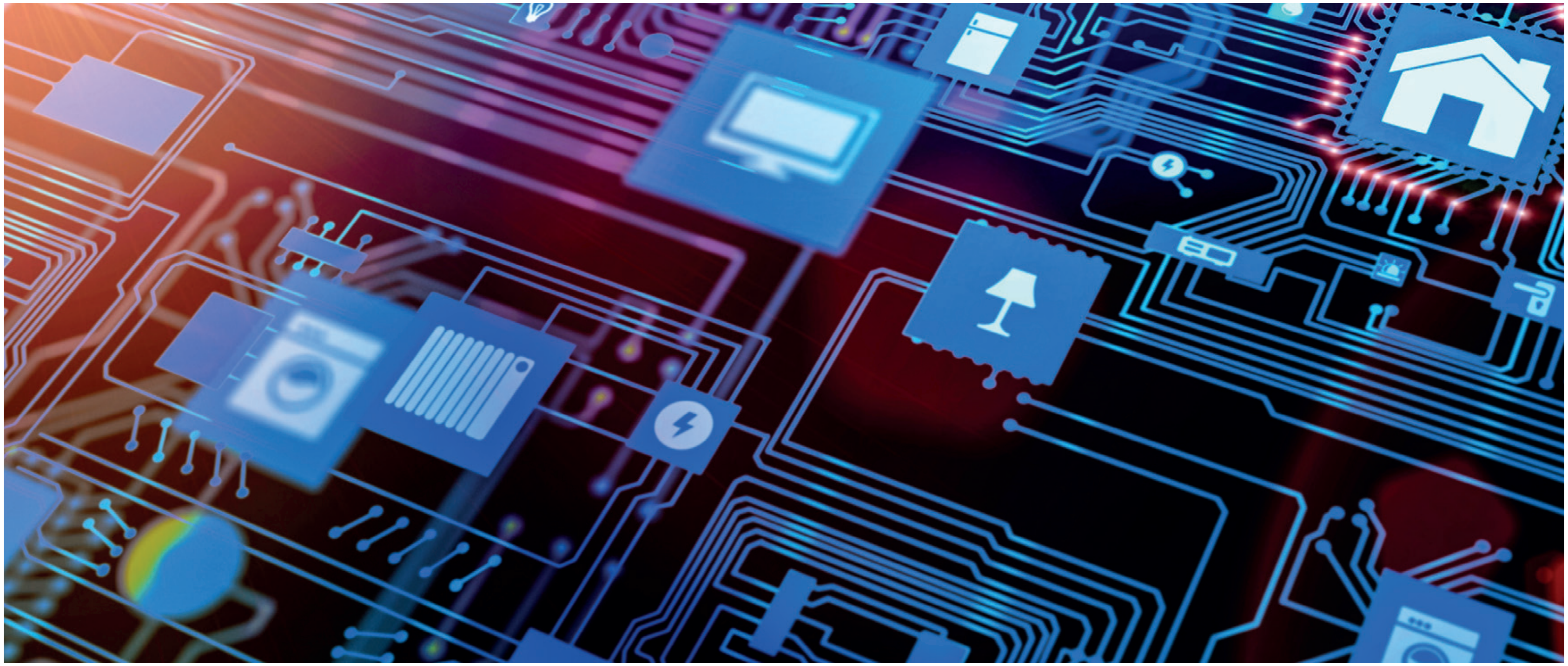
Congratulations! You are now Head of Cybersecurity.

As our digital environments continue to expand we need to find ways to manage and control our data and digital devices. Not just in the more secure (and supported) setting of the workplace but at home.

Away from the office, where we are often protected by layers of professional and digital security we need to start thinking of ourselves as the 'head of cybersecurity' of our own homes.

Many of us now have several, internet-enabled devices, digital storage media and communication tools in our living spaces. In order to keep our data, and our identities, secure we have to find effective ways of administering access because, at home, the responsibility is ours.

Fidelity™ INTERNATIONAL



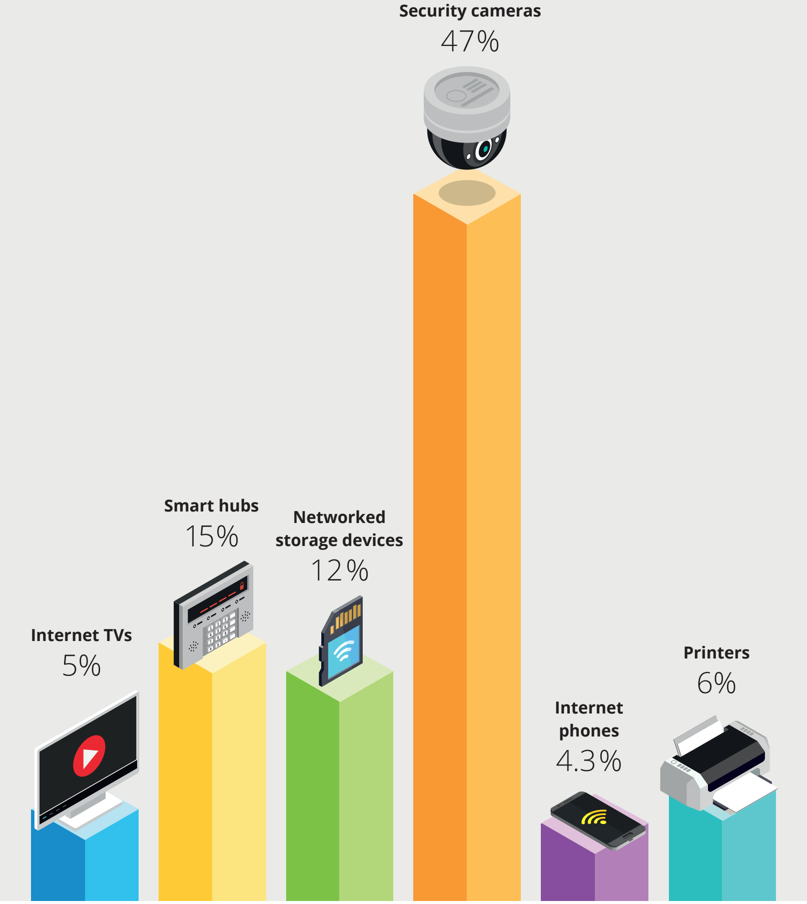
Smart security for the smart home.

The idea of the modern ‘smart home’ and the proliferation of the so-called Internet of Things (IoT) has brought devices into our properties which can be every bit as powerful as those we use at work; enabling automation, enhancing creativity and bringing us previously unimagined levels of convenience. From super-fast WiFi networks, thermostatic sensors and digital security cameras to media-streaming tools and voice-activated apps that proliferate our living spaces there are more opportunities than ever for us to take advantage of the power of the internet in everything, from door-bells to refrigerators. However, the downside of all this accessibility is a significant increase in potential vulnerability. Yes, our always-connected equipment confers huge advantages, but we also need to acknowledge that the smarter and more powerful our home devices get, the more attractive they may become to criminals.

Smart home security. IoT devices most at risk.

These days security doesn't stop at the front door, each of these devices, no matter how useful, is vulnerable to attack. Of investigated attacks between 2018-19 this chart shows the most vulnerable devices targeted by hackers in the internet-enabled household.

Source SAM Seamless Network, Threat Assessment Lab.



Who's watching who?
Security camera systems are revealed as clearly the most hacked smart-home devices. Many of the more affordable models have similar builds and vulnerabilities, allowing hackers to use exploits found in one device to access a range of similar designs. *Omri Mallis*, chief product architect at *SAM Seamless Network* called the cheaper versions "Very vulnerable devices..."

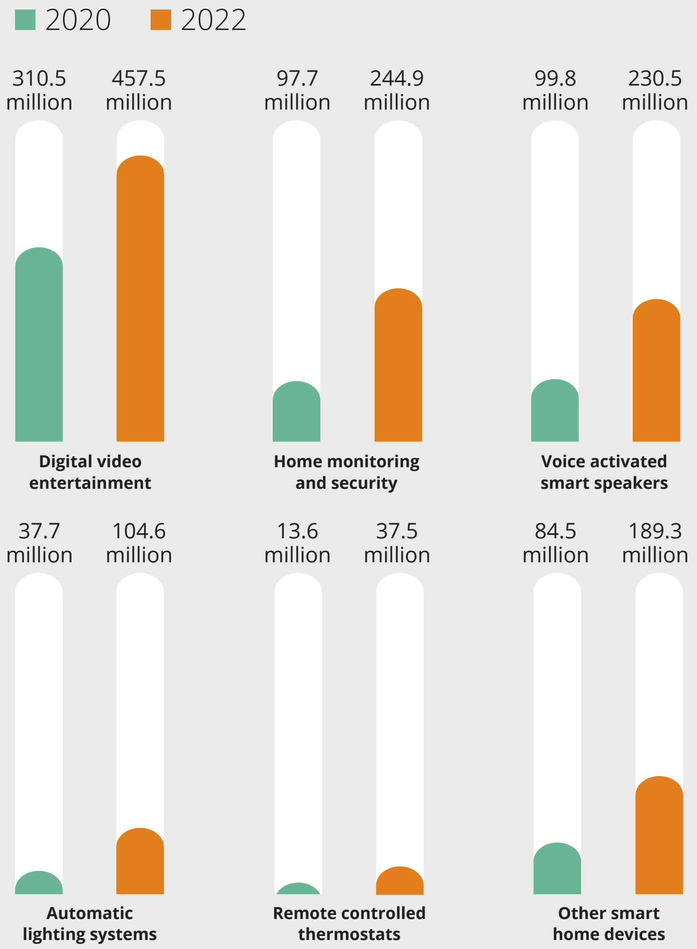
Internet enabled devices are increasingly being singled out as a low-risk, high-reward target for the cyber-aware criminal. It is ironic, for instance, that many of the digital tools which we use to secure our homes from physical incursion, like security cameras, can represent the weak point for a criminal and could potentially leave us exposed to both a loss of privacy and of property.

But it's not just the obvious devices that can lead to danger. It's easy to see how a compromised security camera could leave your security open to abuse, but sometimes the risks aren't so clear. Imagine, for instance, if your home's smart thermostat was hacked, it would be a simple and effective way of seeing when you were away from home for a few days. An ideal time for a burglary.

Most of us will be used to thinking about cybersecurity for our computers, tablets and phones but smart-home security is just as critical. Many IoT devices have vulnerabilities that could allow them to be remotely accessed or controlled over the internet, and our relative unfamiliarity with such equipment means customising settings, updating software and adding security features can present more of a challenge.

Predicted smart home technology growth.

Worldwide smart home device take-up by category in million units.

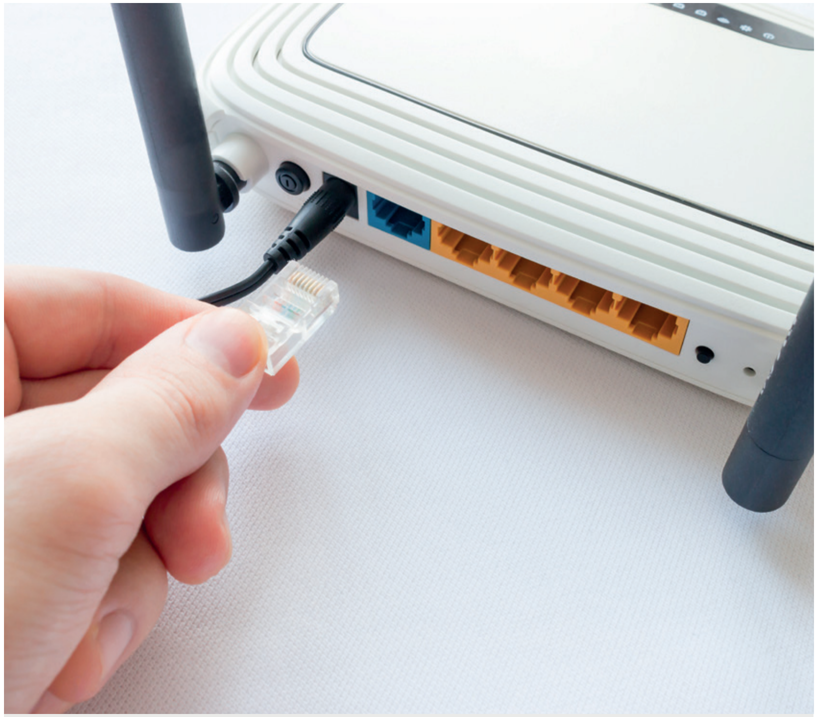


Source International Data Corporation "Market for smart home devices is poised for strong growth"

Accelerating growth

With digital TVs and voice-activated, always-connected devices achieving mainstream adoption, the internet-of-things smart home is no longer the vision of the future. A recent forecast from the International Data Corporation (IDC) shows that the market for smart home devices will see exceptional growth over the next few years. All market segments are expected to at least double in size over the next two years.

In the following pages we'll have a closer look into some of the most-hacked devices and see if we can help you become more aware of the potential issues and vulnerabilities and give you at least some of the knowledge you need to help protect your home, your identity, your data and yourselves.



Routers.

A router creates a link to, and communicates with, your home WiFi using built-in antennas. As a result, all the devices on your home network have internet access. Routers are the essential component of your home's wireless network but they are also full-fledged computers in their own right, complete with operating systems, software... and vulnerabilities.

Router Security. The Tips.

Your home router is your online front door which allows all your devices to connect to the internet so it's really important that you ensure it remains secure. Here are some top tips on how to protect your router. See the 'links' page of this booklet for more information and some step-by-step guides.

Always change the admin password the one set by the manufacturer can easily be discovered by attackers. Getsafeonline.org have provided a step by step guide on how to do this for three of the top Internet Service Providers (ISPs) Virgin, BT & Sky. Just visit their site and click *Protecting Your Computer*.

Turn off service set identifier (SSID) broadcasting - SSID is the name of your wireless network, unless you turn off broadcasting this will be shared to surrounding devices making your network visible, and easily accessible.

Consider setting up a separate 'guest network' for visitors. 'Guest Network' is a feature in most routers and is quick and easy to enable, but make sure you use a different network name and secure password.

If you have children, take advantage of the parental controls provided by your Internet provider. These allow you to restrict access to certain types of websites and set curfew hours for certain gadgets.

Make sure your router's firewall is up and running. A firewall controls network traffic to and from a computer when it's enabled communication between the Internet and your home network is protected.

Home video security.

Having a video-enabled front door camera can be an extremely effective (and comforting) security aid, allowing you to instantly see, in full colour and high-resolution, whoever is ringing your bell, even if you are hundreds of kilometres away. For many years CCTV has been used to prevent crime and identify wrongdoers but now hackers are able to intrude into networks using the same cameras installed to deter them.

Smart camera enabled devices. The Tips.

Smart cameras in the home, like security cameras, baby monitors and so on, generally use your personal WiFi to connect to the internet, allowing you to watch and record live action footage and receive instant alerts. Just like any internet-enabled device, though, you need to take steps to prevent criminals from turning one of the most powerful security tools into one of the most intrusive. These tips will help.

Control who has access to view stored videos and receive alerts. Adding shared users is better than sharing your log-in details, although you should regularly review and revoke permissions when access is no longer required.

Keep the software on these devices up to date to ensure they are protected against the latest security vulnerabilities. If available, switch on the option to install software updates automatically, updating to the latest operating system can improve security and open up new features.

Regularly check and delete camera recordings and logs to see who is accessing the data, and ensure you are complying with local regulations and, where appropriate, letting visitors know if they are being recorded!

If your camera comes with a set, default password, change it to a secure one. You can often change the password using the app you use to manage your device. When you chose a new password, make it a strong one. For plenty of advice on creating easy to remember, hard to crack passwords please see the ‘links’ page at the back of this booklet.

Opt out of third-party data sharing to stop your privative information being available to other service providers.

Internet of Things devices.

The Internet of Things is made up of devices that connect together and communicate with automated systems in your home or on the internet. Each device collects data for a specific purpose and is in charge of a discrete action, from your smart refrigerator ordering milk when it senses you are running low to your television automatically selecting and streaming the next episode of your favourite drama.

IoT smart device security. The Tips.

Every smart device needs to be protected and updated over time as new vulnerabilities emerge. Regrettably some people don't take the time to set them up properly, let alone maintain them. The more our devices know about us the more helpful they can be, but that can also raise issues of privacy if the data falls into the wrong hands.

Change the default user names and admin passwords - these factory-set configurations are easily discoverable so make sure you change them and set a strong, unique password of your own. If the product doesn't allow you to change passwords then you may well want to choose another!

Always set up two-factor authentication if the equipment or app offers it to add a powerful additional layer of security. For more on this two-factor authentication see the 'password booklet' link at the end of this volume.

Check the default privacy settings on the device to check they are set to your liking. In the past few years smart devices have taken data collection to frightening new heights so ensure they aren't sharing your data with other parties or applications without your explicit knowledge and permission.

Keep updated with the latest software updates and operating-system patches to ensure you remain protected. Many devices will update automatically but it's worth checking.

Do your research before you buy, smart devices can collect a lot of data so ensure you know how it's stored and protected. Just like any product, some will be designed with more competence and made with more integrity than others.

Smart speakers and virtual assistants.

Virtual assistants, like Siri, Alexa and Google Assistant, whether accessed through our phones, in the cloud or via propitiatory smart speakers like Sonos, Amazon Echo or Google Nest have become extremely popular in recent years. They enable us to do a variety of things, from controlling lighting systems to online shopping, delivering weather forecasts to streaming music, all at the sound of our voice.

Microphone-enabled devices. The Tips.

We should be aware that we have implicitly given our voice-activated assistants round-the-clock permission to eavesdrop on us. It is their purpose to listen and wait for an activation word or phrase but how frequently do we turn them off when we don't want, or need them? By using virtual assistants to do our online shopping, organise our lives and control our houses we run the risk of their creators learning sensitive, personal information about us. Here are some things to think about before we fill our homes with these devices.

Check, and, if necessary, change the supplied passwords. Often these are not set with security in mind so chose your own.

They are always listening so protect your privacy. Disable the microphone to stop your data being collected (and use the remote instead!) when you don't directly require their functionality.

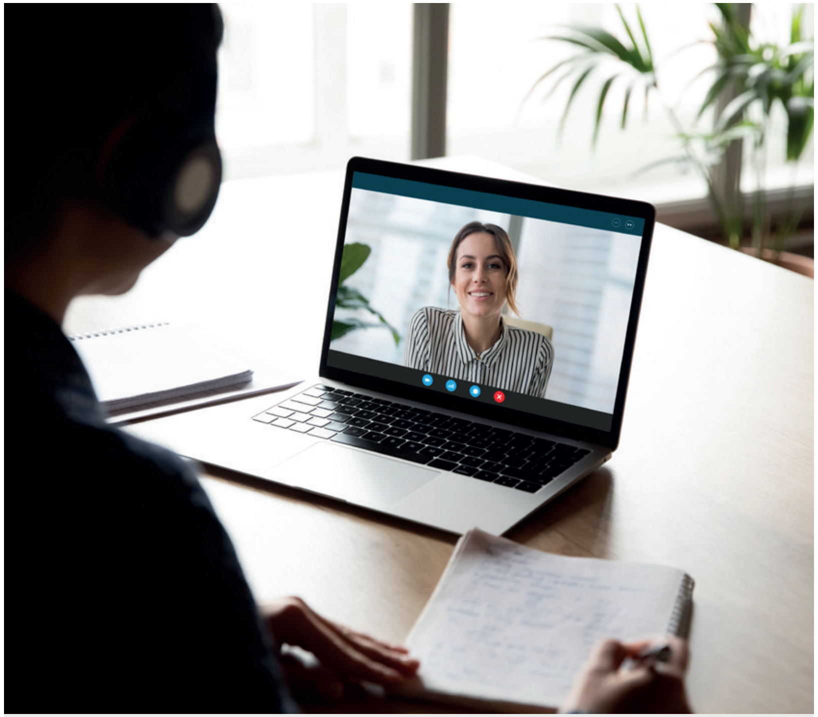
Consider disabling smartphone-sharing which allows your device to send messages and emails using your voice command. Although it sounds like a good idea you could accidentally dictate a message whilst talking and send the conversation to someone you've mentioned!

Disable voice purchases or create a personal identification number (PIN) to ensure you, or others sharing your environment, don't make accidental or unauthorised purchases.

Designate 'microphone-free zones' where you have no smart speakers.

Opt out of transcript recording to prevent your smart speaker from capturing spoken data and sharing it's details with your devices' manufacturer.

Regularly review and delete your communications logs and data.



Computing and communication devices.

Playing video games, word processing, doing homework, programming... these are all still major applications for computing devices in the home, but now they are used for so much more. And let's not forget, these days more and more of us are using our homes as offices too. That being the case it's vital we protect any computer, phone, tablet or device that we use at home.

Computers, tablets and phones in the home. The Tips.

Don't say, "It won't happen to me." All of us know someone who has been on the receiving end of a phishing attack, or had their identity stolen - we're all at risk, personally and financially. Following the tips below, and remaining vigilant, will be a good start to securing your computing devices and protecting yourself. See the 'links' page of this booklet for more.

Install security software like a personal firewall and anti-virus to help protect your devices, apply security patches and keep operating systems up-to-date.

Always use strong, unique, long passwords and PINs for access into devices as you can. For advice on setting powerful passwords and PINs see the 'links' page at the back of this booklet.

Using a Virtual Private Network (VPN) will help to secure data in transit.

Only use Bluetooth to pair with devices you know and disable it when not in use. It can be hacked by those outside your home and used to gain access to your device.

Be careful which websites you visit and links you click on to avoid infecting your device with malware and allowing unauthorised access to your data. Where possible set up multi-factor authentication on any sites you sign up to.

Be constantly aware of phishing scams cyber-criminals will attempt to trick you into divulging personal information, such as your login ID and password, banking or credit card information. If in doubt don't click!

Always dispose of unwanted or old equipment securely ensure you erase the hard disk (using a dedicated file deletion program).

Fidelity™ INTERNATIONAL

Digital security. The Links.

Below you can find links to sites with lots more information and help on the devices and topics we have covered in this booklet. Take a moment to look through them, visit a few, and hopefully you will be inspired to put some of the advice you find there into action. We promise you it will be time well spent.

Routers.

Changing passwords.
A step by step guide to changing wireless passwords on three of the top ISP providers. Getsafeonline.org

In-depth router security.
A very comprehensive, but easy to understand, guide to your router's security settings and where to find them. Lifehacker.com

Firewalls.
Hardware and software firewalls discussed. What they are, what they do and why you need one. Howtogeek.com

Securing your router.
A short, helpful video from the UK City of London police. Youtube.com

Passwords.
A guide from Fidelity to creating strong passwords, passcodes and PINs. ToBeConfirmed.com

IoT and smart devices.

Universal advice.
General guidance for smart devices in the home. Getsafeonline.org

Set-up and manage devices.
Using everyday, network-enabled devices safely. NCSC.gov.uk

Home video security.

Securing home cameras.
How to protect 'smart' security cameras and baby monitors from cyber attack. NCSC.gov.uk

Chosing your camera.
A comprehensive article (and eye-opening video) on the dangers of choosing cheap or badly made security cameras. Which.co.uk

Smart speakers.

Remote working.
A guide to securing your smart speaker when working remotely. Metacompliance.com

Voice assistants guide.
All aspects of voice assisted devices covered. Symantec.com

Computing devices.

Securing your devices.
Check your devices are as secure as possible. NCSC.gov.uk

Has your security been breached?
Check if your account has already been compromised. Haveibeenpwned.com

Staying secure online.
Guarding your personal and financial safety. Fidelity.co.uk

THE END.

Information contained in this booklet has been obtained by Fidelity International from public sources. Care has been taken by the staff of Fidelity International in compilation of the data contained herein and in verification of its accuracy when published, however the content of this booklet could become inaccurate due to factors outside the control of Fidelity International and this booklet should, therefore, be used as a guide only.

This booklet is published and distributed on the basis that Fidelity International is not responsible for the results of any actions taken on the basis of information contained in this booklet nor for any error in or omission from this booklet. Fidelity International expressly disclaims all and any liability and responsibility to any person in respect of claims, losses or damage, either direct or consequential, arising out of or in relation to the use and reliance upon any information contained in this booklet. Fidelity International means FIL Limited and/or its subsidiaries.

Fidelity™
INTERNATIONAL