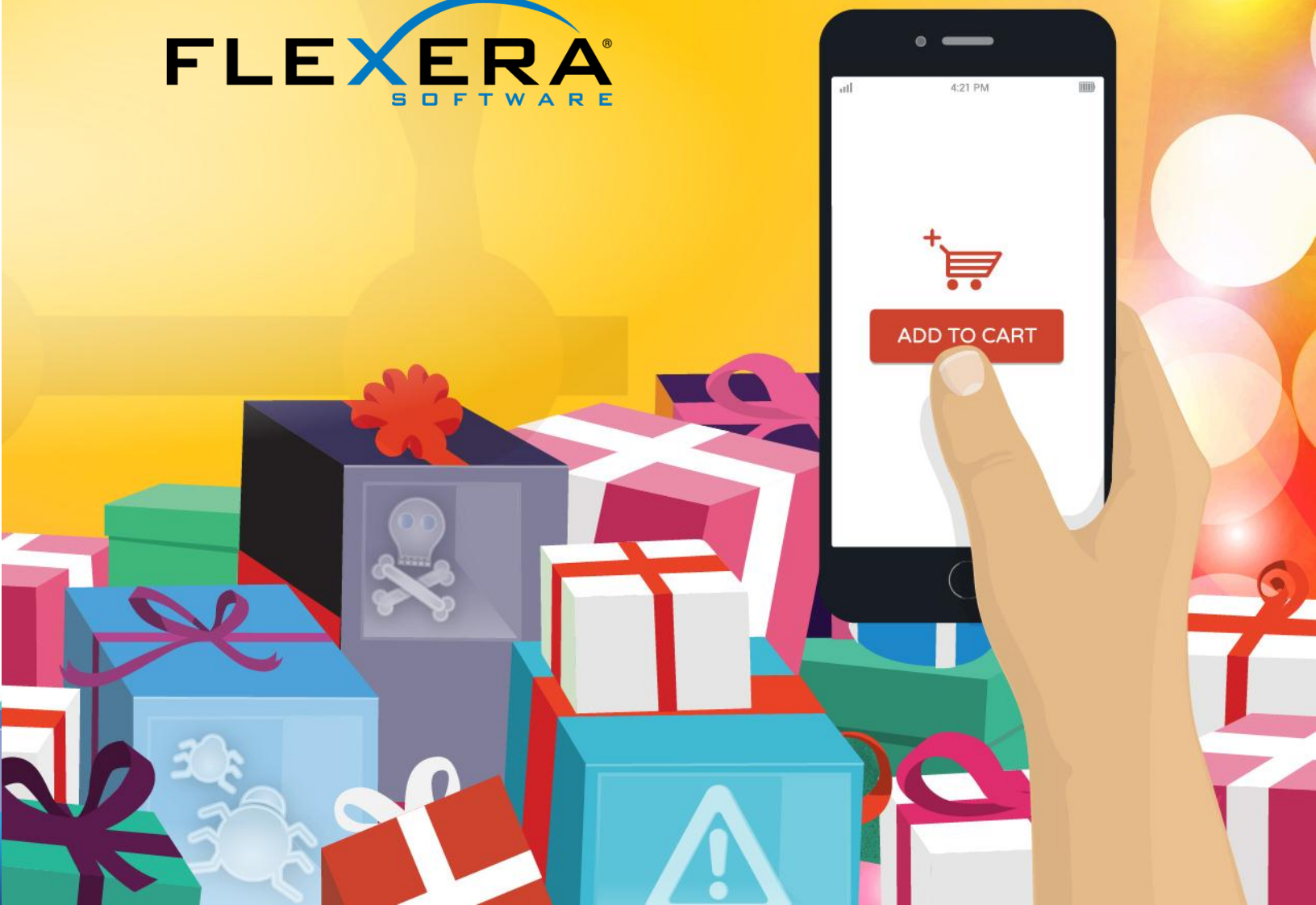
HOLIDAY HAZARD:

Shopping Apps Highlight Risks of Mixing Personal Apps and Business Data

A Mobile App Risk Assessment Report by

FLEXERA® SOFTWARE



Contents

Holiday Hazard: Shopping Apps Highlight Risks of Mixing personal Apps and Business Data

A Mobile App Risk Assessment Report by Flexera Software

Introduction

With the rapid infusion of mobile devices within the enterprise and the growing adoption of company-issued and Bring Your Own Device (BYOD) – mobility is a focal point for containing security risk. As is understanding the risks introduced by mobile applications to sensitive data and company reputation.

Consider a seemingly innocuous mobile phone flashlight app. A Federal Trade Commission lawsuit revealed that a flashlight app maker was illegally transmitting users' precise locations and unique device identifiers to third parties, including advertising networks.

Or consider the Environmental Protection Agency's (EPA) embarrassment when an employee playing on a Kim Kardashian Hollywood app tweeted out to the EPA's 52,000 Twitter followers, "I'm now a C-List celebrity in Kim Kardashian: Hollywood. Come join me and become famous too by playing on iPhone!" What happened? The employee was using the Kardashian app on her iPhone. Unbeknownst to her, the app had the ability to automatically access the phone's twitter account and tweet out messages when certain game thresholds were reached. Unfortunately for the EPA – the phone was configured to use the EPA's official twitter account – not the employee's.

Mobile app security risk is not limited to malevolent hackers and unfriendly governments. Threats to corporate data and reputation can be hidden in the most seemingly innocuous apps, and can be unleashed on the organization by the most well-intentioned employee.

Because of these hidden risks, enterprises must understand the risky behaviors associated with mobile apps that could compromise data security.

Holiday Shopping Hazards on Corporate & BYOD Devices

When the holiday season approaches, even the most serious, focused employees start thinking about gift-giving. And the proliferation of mobile devices has made holiday shopping quick and painless. From Amazon to Walmart, Macy's to Groupon, virtually every retailer – be they brick-and-mortar or online-only – has an app to lure consumers to spend their holiday budgets with them.

Given the proliferation of employer-issued mobile devices and employee-owned devices authorized to access an organization's network (BYOD), many of the season's most popular holiday shopping apps are loaded on devices that also contain highly sensitive, confidential data.

It is therefore incumbent upon IT teams to understand what popular mobile apps their employees are letting onto corporate and BYOD devices, and understand what risks those apps might pose. Testing mobile apps to discover their behavior and risks should be part of any organization's centralized Application Readiness processes.

We examined 26 popular shopping apps available in the Apple App Store to assess them for potential BYOD risk to organizations, including:

- Amazon
- BestBuy
- Banana Republic
- Disney Store
- eBay
- Etsy
- Express
- Gap
- Groupon
- Ikea
- LivingSocial
- Macy's
- Nordstom
- PriceJump
- RedLaser
- REI
- RetailMeNot
- Rue La La
- Shop Advisor
- Shop Savvy
- ShopStyle
- ShutterFly
- Starbucks
- Target
- Trunk Club
- Walmart

We ran tests on these apps using Flexera Software's AdminStudio Mobile which helps organizations identify, manage, track and report on mobile apps, simplify mobile application management, reduce mobile app risk and address the rapidly growing demand for mobile apps in the enterprise.

AdminStudio Mobile tested these apps to determine whether they interact with an Apple iOS device's:

- Ad Network
- Address Book
- Bluetooth
- Calendar
- Camera
- In-app Purchasing
- Pictures
- Location services
- Reminders
- Sharing functionality
- SMS/Texting
- Social Networking
- Telephony

A description of what the test results mean and their potential risks to the enterprise can be found in the Test Descriptions section of this report. There are thousands of shopping apps available in public app stores that employees could download to their corporate-issued or BYOD phones. The results highlighted in today's report with this sampling of popular shopping apps underscores the importance of knowing what those apps do and how they could interact with sensitive corporate data.

Test Result Highlights

Of the 26 popular Apple iOS shopping apps tested:

- All except for Banana Republic and Trunk Club are capable of accessing an Apple iOS device's GPS location tracking service.
- 69 percent, including Amazon, Disney Store, eBay, Groupon, Macy's, Nordstrom, REI, Shutterfly, Starbucks and Target, are capable of accessing an Apple iOS device's social media apps.
- Banana Republic, Gap, IKEA, Savings.com, Target and Trunk Club are the only holiday shopping apps tested that don't support ad networks and therefore would not subject organizations to risks associated with ad networks.
- 65 percent, including Amazon, Best Buy, Disney Store, eBay, Groupon, Macy's, Nordstrom and Walmart, are able to gain access to an iOS device's calendar
- 65 percent, including Amazon, Best Buy, Disney Store, eBay, Macy's, REI, Starbucks, Target and Walmart are able to gain access to an iOS device's address book.
- 58 percent, including Amazon, eBay, Etsy, Groupon, Macy's, Nordstrom, Shutterfly and Walmart are able to gain access to the iOS device's SMS messaging features.
- Of the shopping apps tested, only Best Buy and RedLaser are capable of accessing the iOS device's camera feature.
- Of the shopping apps tested, only Amazon is capable of accessing the IOS device's share feature.

Test Results in Detail

Mobile App	Ad networks	Address book access	Bluetooth LE	Calendar access	Camera	In-app purchasin	Location tracking	Share	SMS	Social networkin	Telephony
Amazon	✓	✓	○	✓	○	✓	✓	✓	✓	✓	✓
Banana	○	○	○	○	○	○	○	○	○	○	○
Best Buy	✓	✓	✓	✓	✓	○	✓	○	○	○	✓
Disney Store	✓	✓	✓	✓	○	✓	✓	○	○	✓	✓
eBay	✓	✓	○	✓	○	✓	✓	○	✓	✓	✓
Etsy	✓	✓	○	✓	○	○	✓	○	✓	✓	✓
Express	✓	○	✓	○	○	○	✓	○	○	○	✓
Gap	○	○	○	○	○	○	✓	○	○	○	✓
Groupon	✓	○	✓	✓	○	✓	✓	○	✓	✓	✓
IKEA Store	○	○	○	✓	○	○	✓	○	○	○	✓
Living Social	✓	✓	○	✓	○	✓	✓	○	✓	✓	✓
Macys	✓	✓	✓	✓	○	○	✓	○	✓	✓	✓
Nordstrom	✓	○	○	✓	○	✓	✓	○	✓	✓	✓
RedLaser	✓	✓	○	✓	✓	✓	✓	○	✓	✓	✓
REI	✓	✓	○	○	○	✓	✓	○	○	✓	✓
RetailMeNot	✓	○	✓	✓	○	✓	✓	○	✓	✓	✓
Rue La La	✓	✓	○	✓	○	✓	✓	○	✓	✓	✓
savings.com	○	○	○	○	○	○	✓	○	✓	○	○
ShopAdvisor	✓	✓	✓	✓	○	○	✓	○	✓	✓	✓
ShopSavvy	✓	✓	✓	✓	○	✓	✓	○	✓	✓	✓
ShopStyle	✓	✓	○	✓	○	✓	✓	○	○	✓	✓
Shutterfly	✓	✓	○	○	○	✓	✓	○	✓	✓	✓
Starbucks	✓	✓	✓	○	○	✓	✓	○	○	✓	✓
Target	○	✓	✓	○	○	✓	✓	○	○	✓	✓
Trunk Club	○	○	○	○	○	○	○	○	○	○	○
Walmart	✓	✓	✓	✓	○	✓	✓	○	✓	○	✓

FLEXERA SOFTWARE® AdminStudio®

iOS Feature Use

This report lists the usage/requirement status of the selected iOS feature(s) for all iOS apps in the Application Catalog. To change the selected feature, or to select multiple features, click **Options** in the toolbar.

Legend

✓ Uses feature

○ Does not use this feature

Test Descriptions

Flexera Software AdminStudio Test: **Ad Network**

- **What does this test result mean?** The app is capable of displaying advertisements "in-app" and connecting to ad networks
- **Potential risk to enterprises:** Online ads frequently come from ad networks that supply code that developers use to insert advertisements into their apps. These ad networks could be vulnerable to hacking, thereby exposing the device and its data to illegal access by a malicious third party.

Flexera Software AdminStudio Test: **Address Book Access**

- **What does this test result mean?** The app is able to access the device's address book.
- **Potential risk to enterprises:** Address books are important to advertisers. If an app is capable of addressing the device's address book, that data could be used by the app developer or shared with third parties such as advertisers, which may violate an organization's privacy, confidentiality or BYOD policies.

Flexera Software AdminStudio Test: **Bluetooth LE**

- **What does this test result mean?** The app is capable of accessing the device's Bluetooth phone features
- **Potential risk to enterprises:** Hackers with specific intent can potentially gain access to data being communicated by the device via Bluetooth communications. If the app in question is capable of accessing private, confidential or sensitive data on the device – and that device's Bluetooth data has been hacked, this could cause a security risk for an organization.

Flexera Software AdminStudio Test: **Calendar Access**

- **What does this test result mean?** The app is capable of accessing the device's calendar and calendar functions
- **Potential risk to enterprises:** Similar to risks associated with apps that access the address book, data from a user's device calendar could be accessed and used by the app developer or shared with third parties, such as advertisers. Given the private, confidential and/or sensitive nature of calendar content – giving apps access to this data may create unwanted security risk depending on the organization and its BYOD policies.

Flexera Software AdminStudio Test: **Camera Tests**

- **What does this test result mean?** The app can access all the device's camera features (including video)
- **Potential risk to enterprises:** Some organizations – especially those operating in high-security environments such as governments, financial institutions, etc. – are extremely sensitive about restricting access to certain sites or locations where employees may take their devices. Accordingly those organization may have policies limiting where/when/how an employee's device camera can be used. If a hacker or malicious third party is capable of hacking into the app – the device's camera could be compromised, potentially exposing confidential or sensitive information. If a mobile app is capable of accessing the device's camera – this may violate an organization's BYOD policy.

Flexera Software AdminStudio Test: **In-App Purchasing**

- **What does this test result mean?** The App enables in-app purchasing
- **Potential risk to enterprises:** In-app purchasing capabilities could expose an organization to unwanted additional costs if the device is tied to a corporate credit card account. An organization might have other software licensing and compliance policies around app procurement that could also be circumvented by in-app purchasing.

Flexera Software AdminStudio Test: **Local Pictures**

- **What does this test result mean?** The app is capable of accessing photos taken by and stored on the device
- **Potential risk to enterprises:** Pictures on phones can contain confidential material, such as sensitive site installations, location and time stamp data. How the app then treats the photos and the associated metadata (like date/time and location), and whether the app uploads or sends photos elsewhere, may pose a data security risk to an organization. Depending on an enterprise's security requirements, this could violate BYOD policy.

Flexera Software AdminStudio Test: **Location Tracking**

- **What does this test result mean?** The app can access the device's GPS location services
- **Potential risk to enterprises:** Confidentiality and privacy concerns in many organizations would prohibit unapproved apps from tracking employee location information. Moreover, to advertisers, location is one of the most valuable things on a device, so many apps access this data solely to pass along to advertisers. Consequently many organizations restrict apps that can access location services on employer-issued or BYOD devices.

Flexera Software AdminStudio Test: **Share**

- **What does this test result mean?** The app is able to access the device's share feature
- **Potential risk to enterprises:** The device's share feature gives users a convenient way to share content with other entities, such as social sharing websites or upload services. Employer-issued and BYOD devices may be linked to corporate social media and other accounts. If the share function on the device is accessed, personal employee data or content could inadvertently be shared to a corporate social media site. Some companies may have policies against allowing apps onto employer-issued or BYOD devices capable of accessing the share function.

Flexera Software AdminStudio Test: **SMS**

- **What does this test result mean?** The app can access the device's text functionality
- **Potential risk to enterprises:** Apps that can access the device's SMS functionality can potentially read text messages that are stored on the phone, or create text messages and send them to recipients – for instance contacts on the device (if the app can also access the contact list). This poses significant potential privacy concerns for corporate-issued or BYOD devices, given that confidential information could be contained in the text messages.

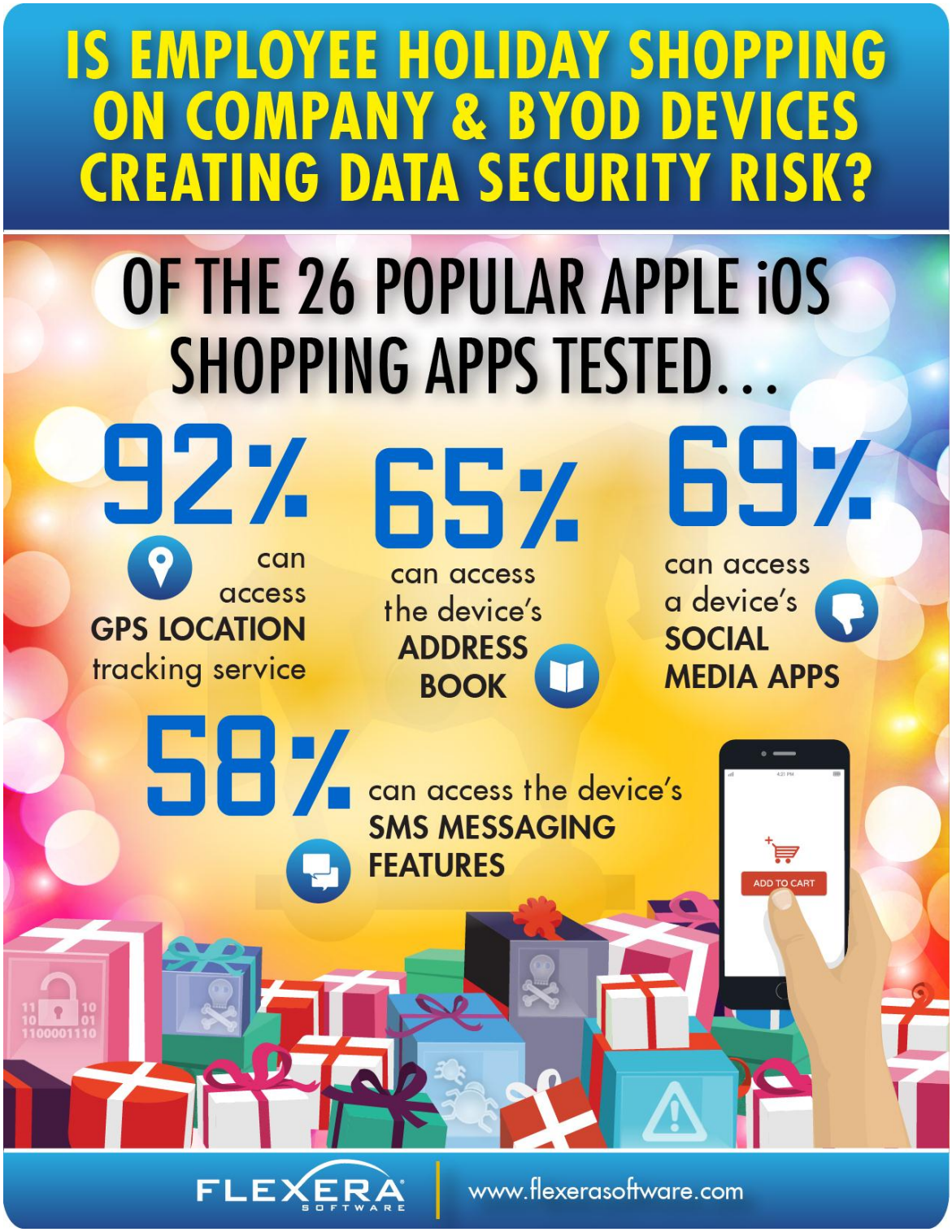
Flexera Software AdminStudio Test: **Social networking**

- **What does this test result mean?** The app can access and share data with social networking sites
- **Potential risk to enterprises:** Employer-issued and BYOD devices often contain confidential information that should not be shared in a social media setting. Apps able to access social media sites could potentially share confidential data. Likewise, a corporate or BYOD device that contains personal employee content could inadvertently share personal data to a corporate social media site linked to the device.

Flexera Software AdminStudio Test: **Telephony**

- **What does this test result mean?** The app can access the devices phone function
- **Potential risk to enterprises:** There is a risk that an app accessing telephony features could call restricted phone numbers or "premium" phone numbers that, for instance charge high fees – such as per-minute calling charges. In some instances, organizations may want to restrict apps capable of accessing a device's telephony function.

Infographic



About Flexera Software

Flexera Software helps application producers and enterprises increase application usage and security, enhancing the value they derive from their software. Our software licensing, compliance, cybersecurity and installation solutions are essential to ensure continuous licensing compliance, optimized software investments, and to future-proof businesses against the risks and costs of constantly changing technology. A marketplace leader for more than 25 years, 80,000+ customers turn to Flexera Software as a trusted and neutral source of knowledge and expertise, and for the automation and intelligence designed into our products. For more information, please go to: www.flexerasoftware.com.

Flexera Software, LLC
(Global Headquarters)
+1 800-809-5659

United Kingdom (Europe,
Middle East Headquarters):
+44 870-871-1111
+44 870-873-6300

Australia (Asia,
Pacific Headquarters):
+61 3-9895-2000

For more locations visit:
www.flexerasoftware.co