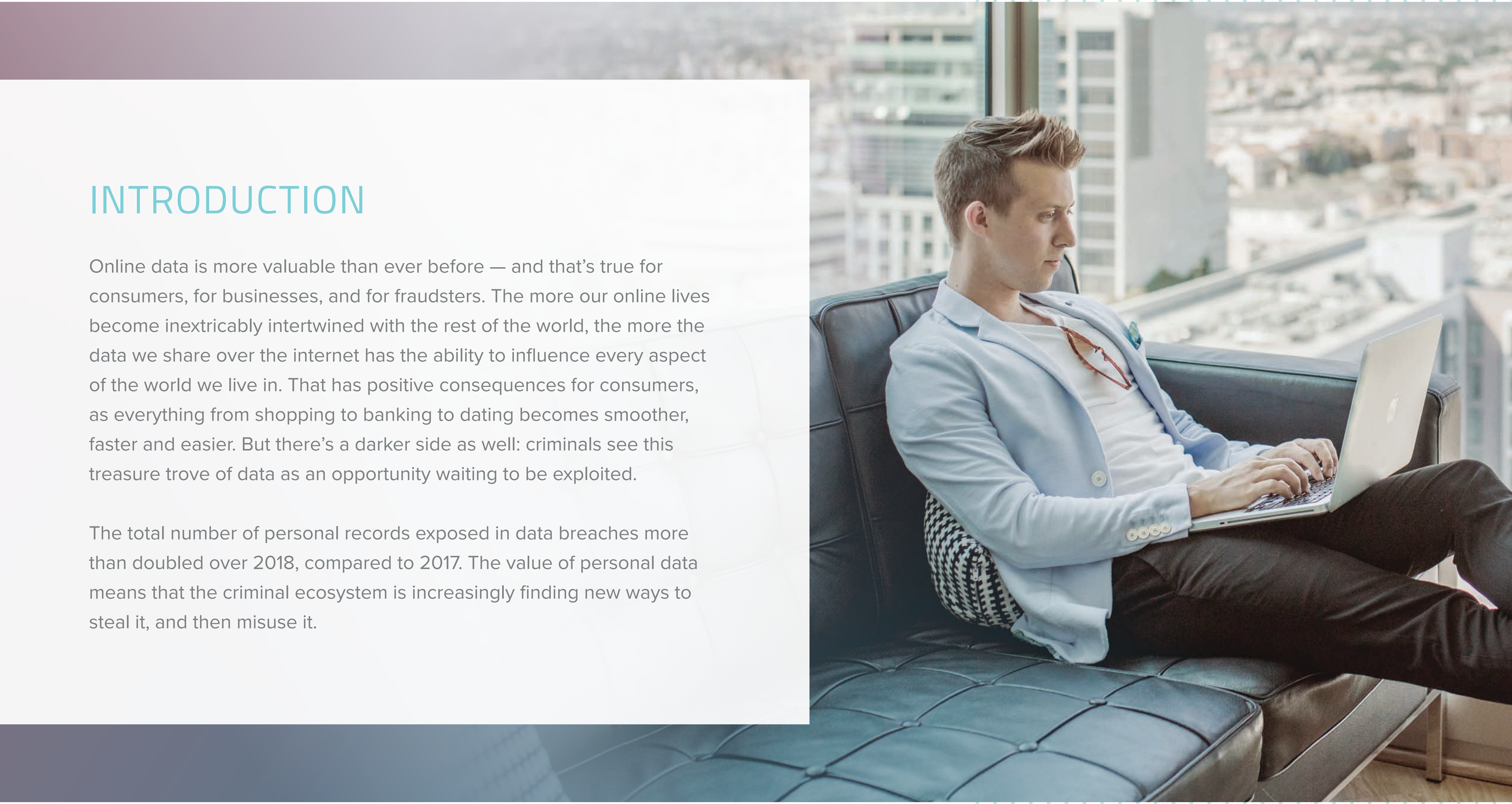
FORTER

INCREASED COMPLIANCE, MORE FRAUD?

The Unintended Consequences of Compliance and What to Do About It



INTRODUCTION

Online data is more valuable than ever before — and that's true for consumers, for businesses, and for fraudsters. The more our online lives become inextricably intertwined with the rest of the world, the more the data we share over the internet has the ability to influence every aspect of the world we live in. That has positive consequences for consumers, as everything from shopping to banking to dating becomes smoother, faster and easier. But there's a darker side as well: criminals see this treasure trove of data as an opportunity waiting to be exploited.

The total number of personal records exposed in data breaches more than doubled over 2018, compared to 2017. The value of personal data means that the criminal ecosystem is increasingly finding new ways to steal it, and then misuse it.

The value of data, and its vulnerability, has led to new legislation and procedures intended to protect information shared and stored online. Europe's GDPR, intended to increase consumer's rights over their own data, became binding in May 2018, and a variant in California is slated to become effective at the beginning of 2020, complicating matters for companies that limited their European data presence in hopes of avoiding GDPR. The revised Payment Services Directive (PSD2), which was devised to both democratize access to data and simultaneously protect it through Strong Customer Authentication (SCA), will come into effect in Europe in September 2019.

Perversely, both GDPR and PSD2, which were created to protect customers and their data, actually introduce new risks and complications for businesses operating online. Companies need to consider their new reality carefully and face the challenge: how do you remain compliant with new legislation while simultaneously remaining secure?

DATA FROM DIVERSE DIRECTIONS

In recent years more diverse types of data have become valuable. Crooks used to focus on information like credit card or debit card details, social security numbers or equivalents, and passport details. While these types of data retain their allure, information such as user names and passwords, purchase history or loyalty memberships, and even biometric data is now equally sought after to build up an accurate picture of an individual's profile, which can be used for fraud. Businesses have a greater need than ever before to know their customers, so that they can distinguish the good from the bad.

THE POWER OF DATA LEADS TO POWERFUL DIRECTIVE

The more our online and offline identities and activities blend together, the greater the value of the data we share. Consumers today tend to prioritize convenience over security. **While a Forter survey found that 72% of those surveyed were concerned about their private details being stolen via a retailer's website,** 50% also admitted that they were less likely to buy if the checkout process took more than 30 seconds, and 56% reported that the more time and effort a purchase required, the less likely they were to complete the purchase.

Retailers have found that despite consumer security concerns, customers will entrust them with their private data in order to make shopping faster and easier. **This results in a heavy burden of trust being placed on the shoulders of businesses in general, and information security professionals in particular.**

The same desire to balance between flexibility and security has played out in recent EU debates and directives. PSD2 has opened up direct access to account data, trying to create a more level playing field for payments companies. Previously, access was generally limited to traditional players such as banks and card networks, and the directive is intended to encourage innovation in order to benefit both consumers and businesses.

Yet, there's a careful balance that must be found between opening up data access to increase the options available to both customers and companies and limiting access to guard data from malicious actors. In the case of PSD2, this has played out through the introduction of Strong Customer Authentication (SCA), which must be employed in the EU when a user accesses their payment account online or initiates a payment transaction. SCA, which can be achieved through mechanisms such as 3-D Secure, protects consumer privacy and data by attempting to ensure that a user is who they say they are.

In a similar vein to SCA, the GDPR legislation aims to give individuals more control over their personal data. It affects how companies can use and process data, the protections they are required to provide for it, and their obligations in the event of a breach. No company operating in the EU or with EU data can afford to ignore it: violators of the GDPR may be fined up to 4% of the annual worldwide turnover of the preceding financial year (for enterprise), or €20 million (for smaller companies).

All of this sounds as though it ought to make life more difficult for criminals. The more protections companies have in place, and the greater the control given to consumers over their own data, the harder things should be for malicious actors. Unfortunately, criminals are nothing if not creative. Online data is exceedingly valuable meaning that for them these obstacles represent challenges rather than deterrents.

DATA: VALUABLE, AND VULNERABLE IN SO MANY WAYS

Data breaches have become such a standard occurence in today's world that many companies have begun viewing a breach as a matter of when rather than if. According to the Accenture "Cost of Cybercrime" report, the average cost of cyber crime rose by over $1M last year to reach $13M per firm. Those surveyed recorded an average of 145 cyber attacks resulting in hackers entering their core networks or enterprise systems: up 11% over 2017 and 67% over 2014.

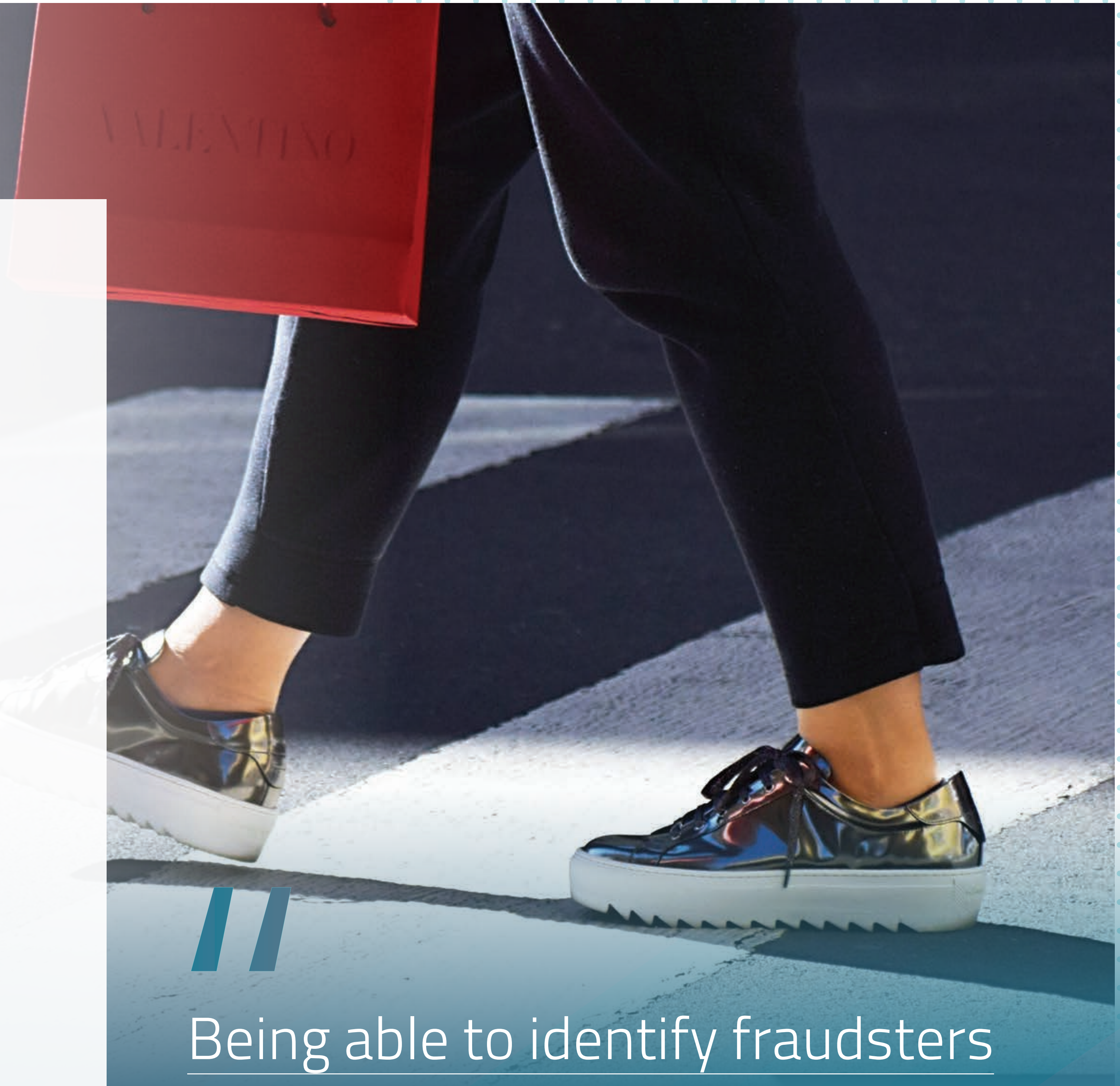
Interestingly, in support of the importance of GDPR and PSD2 in Europe, the 2019 M-Trends report found that EMEA countries were particularly weak when it comes to dwell time — the amount of time it takes to report a hack. **While the average dwell time in the Americas was 71 days and the global median 78 days, in EMEA the average was 177 days.** The pressure is on and mounting for infosec professionals everywhere in the world, but those in EMEA are especially in the spotlight with the need to remain compliant and defend against bad actors.

Unfortunately, the more data that is made available to the criminal fraternity, the easier it is for clever fraudsters to present themselves convincingly as one of their victims. The more information stolen about a customer's buying patterns, accounts and even biometric or passport data, the easier it is to pretend to be that customer.

> Forter's Sixth Fraud Attack Index found that fraud rings increased by 26% over 2018.

SPOTLIGHT ON SOPHISTICATION

The online criminal ecosystem is increasingly sophisticated, meaning that it gets easier all the time for crooks to leverage stolen data in a way that is efficient, effective and scalable. **Forter's Sixth Fraud Attack Index found that fraud rings increased by 26% over 2018.** In a fraud ring, each actor has a criminal specialty, whether it is stealing information through phishing, seeking out technical vulnerabilities on a website, social engineering, or creating legitimate-looking purchases using a hacked account. Working in tandem allows such groups to scale their attacks, and their diverse expertise makes them more likely to succeed. Moreover, automation in the form of bots is increasingly popular with both fraud rings and individual fraudsters, dramatically increasing the speed and scale of attacks. All of this makes bad actors harder to keep up with, harder to spot, and harder to stop.



THE LAW OF UNINTENDED CONSEQUENCES

“No battle plan survives first contact with the enemy.” This axiom is just as true in the war against cyber crime. Both GDPR and PSD2 were born of good intentions and a desire to protect data and consumers’ rights over their own data. But today’s payments ecosystem is intricate and complex, and it is hard for legislation to predict and guard against the moves criminals will take in reaction to it.

With GDPR, consumers can request deletion of their data at any time. For fraudsters, this is practically a license to print money. If they can disguise themselves as legitimate actors, they can demand all data on their personas be removed, and present themselves to online businesses as blank slates every time. **Being able to identify fraudsters as returning bad actors is vital to all fraud fighting efforts,** and not having previous visits to draw on would be a serious handicap to fraud prevention.

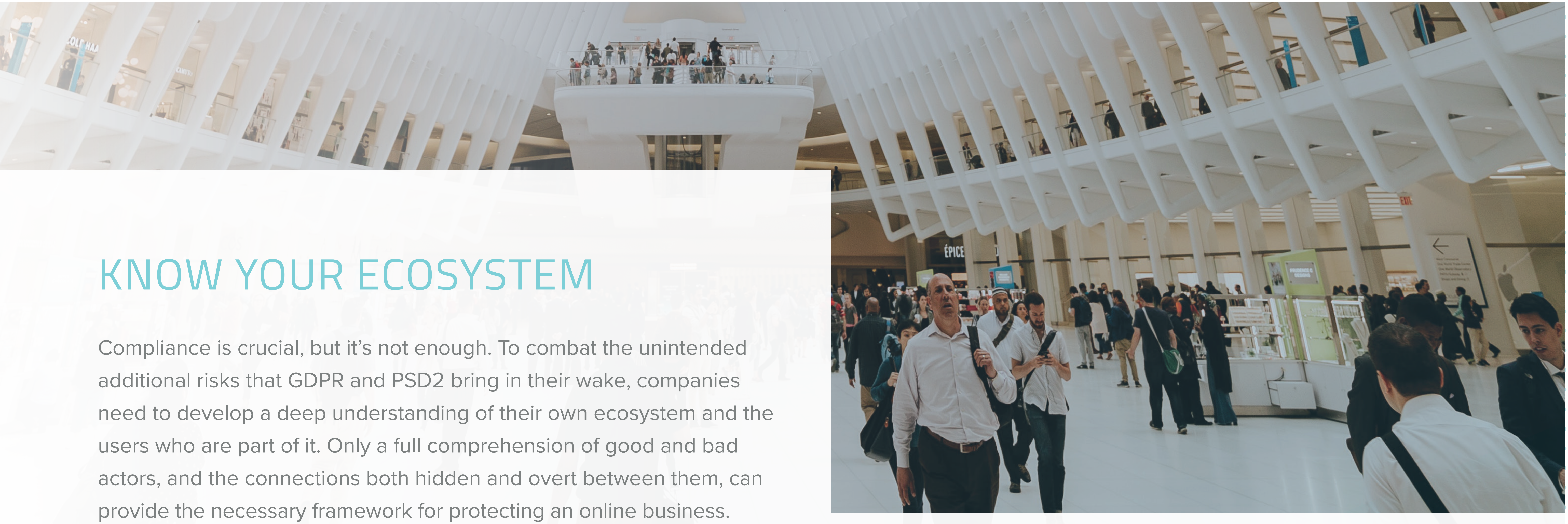
> Being able to identify fraudsters as returning bad actors is vital to all fraud-fighting efforts.

In the case of PSD2, an unintended consequence is similar to the unfortunate side effect of EMV introduction. In that case, fraudsters were successfully deterred from carrying out card present fraud, and shifted online to card not present fraud instead. With PSD2, making fraud more difficult at the point of transaction within EU transactions is likely to shift fraud to other geographies and attack points.

Most online businesses are global, and those that sell outside the EU, as well as within it, will have to be particularly careful of non-EU transactions once PSD2 kicks in. Criminals who stop using European data won't stop stealing; they'll just start using data from elsewhere. Businesses who have traditionally focused their fraud prevention efforts on the EU must make sure they expand their analysis globally, in order to protect against the shifting threat.

Similarly, fraudsters blocked from the point of transaction won't give up. They'll attack other points in the customer journey such as taking over accounts to steal data, use gift card credit, or leverage loyalty points.

> Criminals who stop using European data won't stop stealing; they'll just start using data from elsewhere.



KNOW YOUR ECOSYSTEM

Compliance is crucial, but it’s not enough. To combat the unintended additional risks that GDPR and PSD2 bring in their wake, companies need to develop a deep understanding of their own ecosystem and the users who are part of it. Only a full comprehension of good and bad actors, and the connections both hidden and overt between them, can provide the necessary framework for protecting an online business.

A rich understanding of your ecosystem mitigates the GDPR risk because the legislation does not require you to delete the information of known criminals. If your system is accurate enough to detect fraudsters reliably, and to make the right connections to recognise them when they return in different guises, then you won’t need to delete their data — even on request. In fact, such a request would simply become additional, valuable information.

It isn’t enough to be able to match obvious data points such as addresses, names or even IP addresses, of course. Only rookie criminals would repeat that kind of detail. Your system needs to be able to match behavioral data and patterns and use cyber intelligence to piece together obfuscated elements. Only then can you identify malicious actors continuously, even when they have changed everything they can in their digital appearance.

A similar level of sophistication and sensitivity is necessary for dealing with the “attack shift” that will likely follow PSD2. **Your system must be able to analyze every aspect of your user experience and journey, not just focus on checkout.** There is no other way to identify and protect against criminals attempting to attack your users’ accounts and loyalty programs.

In order to guard against the risk of a geographical fraud shift, your system must be sensitive to the genuine behaviors of different geographical areas, and be able to flag when a user does not match the expected norms for their location. Different industries and businesses have different behaviors, and so it is vital that your system be attuned to your own ecosystem. This is not at one size fits all problem; your ecosystem is not the same as any other, and to protect it you need to understand it in all its unique complexity.

> Your system must be able to analyze every aspect of your user experience and journey, not just focus on checkout.

Make sure your customers and accounts are protected by a system that knows your ecosystem just as well as you do. It requires flexibility and continuous innovation, and an ongoing effort to stay ahead of criminals, and abreast of the evolution in customer behaviors and expectations. However, with constant, accurate, informed protection, you can maintain compliance, security, and your customers’ precious trust.

About FORTER

Forter's fraud prevention solution protects online merchants from fraud attacks and abuse at both the account level and the point of transaction, while maintaining a seamless customer experience. By evaluating more than 6,000 data points, Forter determines the legitimacy of each individual that comes into contact with a retailer's site. We are powered by a unique blend of artificial intelligence and ongoing human research, resulting in exceptionally accurate fraud protection, more sales and happier customers.

For more info visit **www.forter.com**