Fraud on the rise: can technology save us?

With the global cost of chargebacks mounting for consumers, banks and merchants alike, Alice Bonasio argues that we need innovation to fight back

Online fraud is now the most commonly experienced crime in England and Wales, according to a report published by the UK National Audit Office (NAO). Up to 1.9 million cyber-related fraud incidents were estimated to have taken place last year alone, with the cost likely to run into billions of pounds.

The report also outlined that the NAO faces a significant challenge in influencing partners, such as banks and law enforcement bodies, to take on the responsibility of preventing and reducing fraud. As a *"low-value but high-volume crime",* fraud is often overlooked by governments, law enforcement, and industry alike, says Amyas Morse, Head of the NAO. Acknowledging that the landscape for tackling online fraud is extremely complex, the report calls for an urgent response to address it.

The report further cites that online fraud is under-reported; even where data is available there is a lack in the sharing of information between government, industry, and law enforcement agencies. In fact, there is no formal requirement for banks to report fraud or share reports with government, yet we see consistent evidence of fraud recurring all over the world. This is an enduring and global problem, one that takes a heavy toll on merchants and service providers of all sizes, as well as banks, issuers, and ultimately customers.

The growing scale of online fraud also suggests that many people are still not aware of the risks, and that there is much to be done to change behaviour. This is also evidenced in separate figures from Citizens Advice showing a 17% rise in consumers being caught out buying 'phantom' goods online. This type of cybercrime occurs when fraudsters advertise items at cut prices on social media sites like Facebook and Instagram—as well as online marketplaces such as Gumtree and eBay—and con buyers into spending on average £1,100 on products ranging from cars to flights and even insurance, which simply do not exist. In only a few months, January to March this year, Citizens Advice logged over 3,600 complaints about such phantom goods.

These scams can have a lasting financial and emotional impact on consumer confidence and their relationship to merchants. While educating consumers is both sensible and necessary, the NAO report stresses that government and industry still have a responsibility to protect citizens and businesses. The report also found that the protection banks provide varies, with some investing more than others in educating customers and improving their anti-fraud technology.

Given that organized attacks of online fraud is likely to increase, this investment is absolutely essential—yet keeping up with the latest techniques employed by fraudsters can put tremendous strain on a company's logistics. While few would argue that fraud detection and prevention is a priority for businesses, the fact is most businesses lack the necessary resources to build and maintain such solutions. It is the industry's responsibility, however, to keep up—and ideally get ahead—of these fraudsters in order to protect both themselves and consumers.

By 2020... card fraud worldwide is expected to reach $31.67 billion

The adoption of such technologies has indeed been shown to have a significant positive impact on fraud prevention. Take, for example, EMV—the technical standard for smart payment cards and terminals that have allowed the rollout of payment solutions, such as Chip and Pin and Contactless. In the UK, its implementation led to a dramatic reduction of 32% in the levels of overall card fraud in the seven years following their introduction in 2004, according to official figures from the UK Card Association.

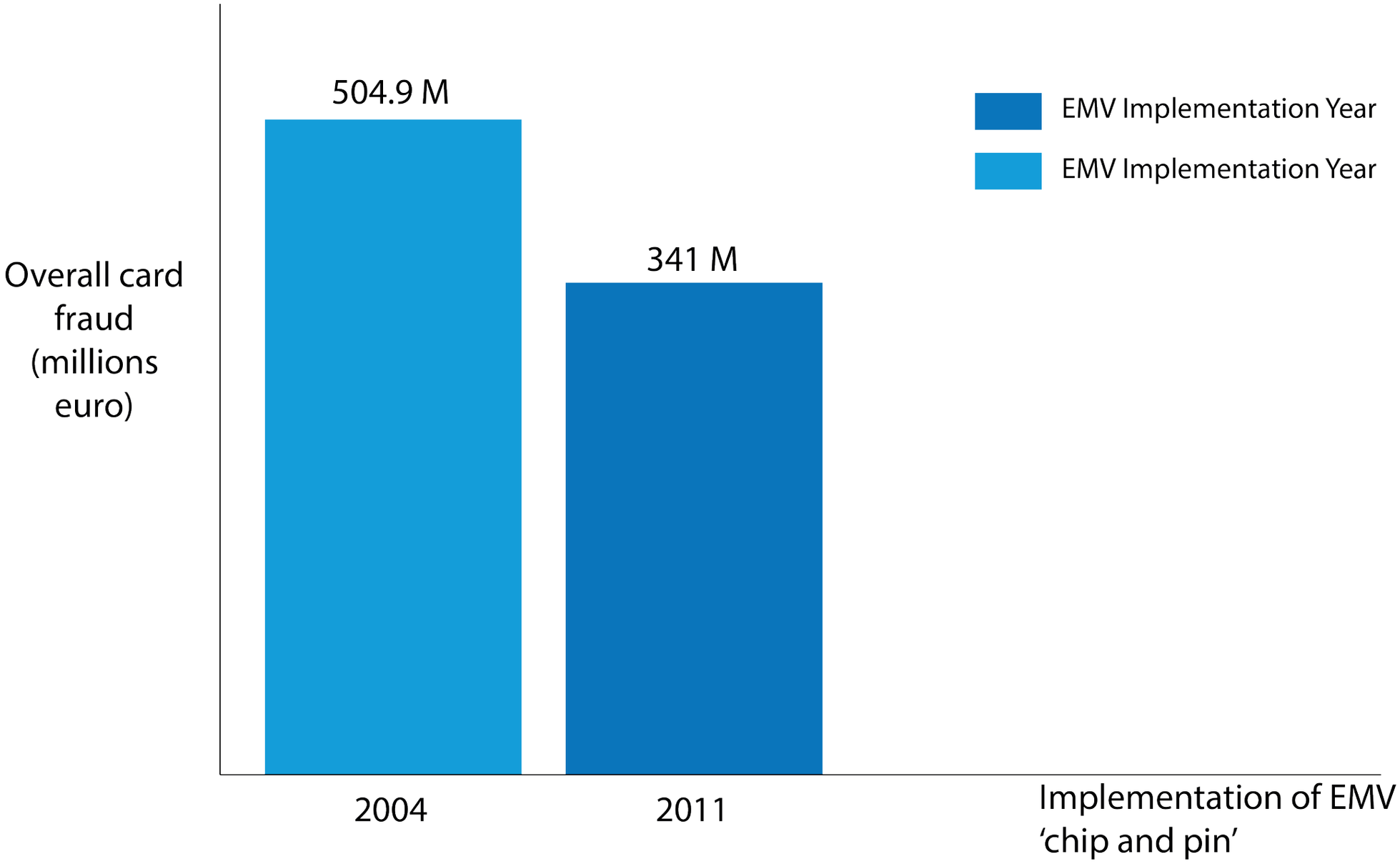
Such measures have undoubtedly made fraud much more difficult to perpetrate in 'card present' payment scenarios, yet the shift to online retail has brought with it an entirely new set of challenges relating to fraud prevention and mitigation. There is no getting away from the fact that individual shopping habits have fundamentally changed over the past decade, and that the shift towards online and mobile shopping is not going to be reversed. PricewaterhouseCoopers' (PwC) *Total Retail 2016 Survey* found that the popularity of mobile shopping continues to rise, stating that *"46% of our global sample buys products via mobile at least a few times a year, compared to 40% last year".*

While this might be good news for consumers in terms of better prices, more choice, and added convenience, it leaves the bulk of 'card-not-present' transactions—which are the norm in online shopping and vulnerable to problems such as chargebacks. These chargebacks happen when customers dispute a transaction in their statement and request a refund—often going directly to their card issuer or bank and bypassing the merchant altogether.

According to *The Nilson Report*, gross card fraud losses for 2015 reached $21.84 billion, not including the costs incurred by issuers, merchants, and acquirers for their operations, call centres, and chargeback management. By 2020, the report concludes, card fraud worldwide is expected to reach $31.67 billion, and that measures such as improving methods of reducing fraud on card-not-present transactions are critical to keeping those losses in check.

This is a complex issue, since there are many factors which can trigger a chargeback in the first place, and a blunt approach can cause a merchant more harm than good. One of these factors is known as 'buyer's remorse'—where

Figure 1. EMV implementation has reduced card fraud



a customer finds a product at a cheaper price elsewhere and uses the system as an alternative returns and refund mechanism. This is one of the forms that so-called 'friendly fraud' takes. Another common scenario is where a person requesting the refund is not entirely sure they haven't made the transaction, but will 'try their luck' anyway. Since the cost of investigating such claims is often much higher than the value of the refund itself, banks will mostly opt to issue the refund without dispute, and some customers have learned to take advantage of this to manipulate the system. According to industry research firm Aite Group in their *Impact Note* of August 2016, 60% to 70% of chargebacks are the result of first-party or friendly fraud.

Business can minimise vulnerability to chargebacks in various ways. These include ensuring that they build a good relationship with their customers, by providing accurate product information and keeping the lines of communication open, so customers are more inclined to approach merchants with queries than to go directly to the issuing banks to initiate a dispute. Having a clear and efficient refunds policy also minimises the chance of experiencing so-called buyer's remorse, where a customer is tempted to use chargebacks as a backup refund mechanism. However, many customers still get confused when seeing an unfamiliar name appear on their statement, as often merchants will be listed under names which differ significantly from their brand or trade name.

"When a customer sees a charge they don't immediately recognise on their card, they often ask the bank to remove that charge from their statement", explains Matthew Katz, CEO of Verifi, a provider of end-to-end payment protection and management solutions. *"This is done by calling the bank directly to raise a dispute, leaving out the merchant who could potentially provide further information to clarify what the charge relates to. In fact, our research has found that up to 86% of cardholders bypass the merchant and contact their issuing bank directly to dispute or question a charge on their bill"*.

While banks generally issue a refund to the customers, the process often has a very negative impact on overall customer experience, causing confusion and lingering trust issues which can lead to future sales being lost. This has

an added impact on the merchant's bottom line, on top of the fees, fines, and operational expenses of handling the chargeback in the first place.

These costs quickly snowball, ranging from administrative resources needed to investigate claims and process refunds, to fielding customer queries and potential loss of legitimate sales, present and future. Add this to the operational expense of preparing and shipping merchandise, as well as the value of the goods themselves which often must be written off, and the cost for merchants quickly adds up. Ultimately, this is also very bad news for consumers, as these costs will eventually trickle down the supply chain and translate into higher prices. The true price of these chargebacks is not reflected in the refund amounts alone, significant as these may be. In their September 2015 report, *The Impact of Fraud and Chargeback Management on Operations*, Javelin Research found that organizations typically spent between 13% and 20% of their operational budget on fraud and chargeback management.

"Globally, chargebacks continue to grow and represent a significant challenge", agrees Katz, *"To address this problem, we need solutions that better align the interests of cardholders, merchants, and issuing banks on a global scale, focusing on continual innovation and refinements that are essential to effectively combat this problem",* he believes.

This is what Cardholder Dispute Resolution Network (CDRN) does, according to Katz. Verifi's solution—which covers approximately 50% of the US market and boasts a 90% resolution rate—was named for the fifth year in a row as 'Best Chargeback Management Program' by CNP Expo. It is now continuing to expand in international markets such as the United Kingdom, Verifi having opened an office in London in 2016, and now announcing a key strategic partnership with payments processor MegaCharge.

One of the problems that CDRN addresses, according to Katz, is the fact that by the time merchants learn of the issue, it's often too late to stop the chargeback. *"Our patented closed-loop technology integrates directly with the top*

issuing banks. This pauses the chargeback process for up to 72 hours and redirects cardholder disputes from the bank to the merchant in near real-time. The merchant will have more time to assess and resolve the dispute before it ever becomes a chargeback. To date, we are supporting more than 25,000 accounts globally and handling over 200,000 individual chargebacks each month—amounting to an estimated $195 million in chargebacks prevented.

"The problem of chargebacks and friendly fraud are not only impacting businesses' bottom line, but hindering future growth and jeopardizing customer retention, trust, and satisfaction rates. For merchants to strengthen their risk management and counter friendly fraud, the ideal line of defense would permit merchants to provide insights into the cardholder's order as shopping cart-level data. This would feature merchant details and even the device used to make the purchase through the financial institution's platform—all at the time the dispute arises. This deeper level of data can help cardholders better understand their purchases and avoid filing false cases of fraud that result in lost sales, higher labour costs and more", Katz concludes.

Since the bulk of consumer purchases will be made online, it stands to reason that to tackle online fraud we must leverage data and technology in increasingly sophisticated ways. As the recent reports on the growing scale of this global problem show, gone are the days when the tools to do so could be considered an optional extra. They have, quite simply, become business essentials for every merchant looking to conduct business in the digital age. ■

Alice Bonasio is a Writer, Academic and Strategic Consultant specialising in Technology and the Creative Industries