THE GROWING ISSUE OF THE COST OF PAYMENT FRAUD

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

IDEX

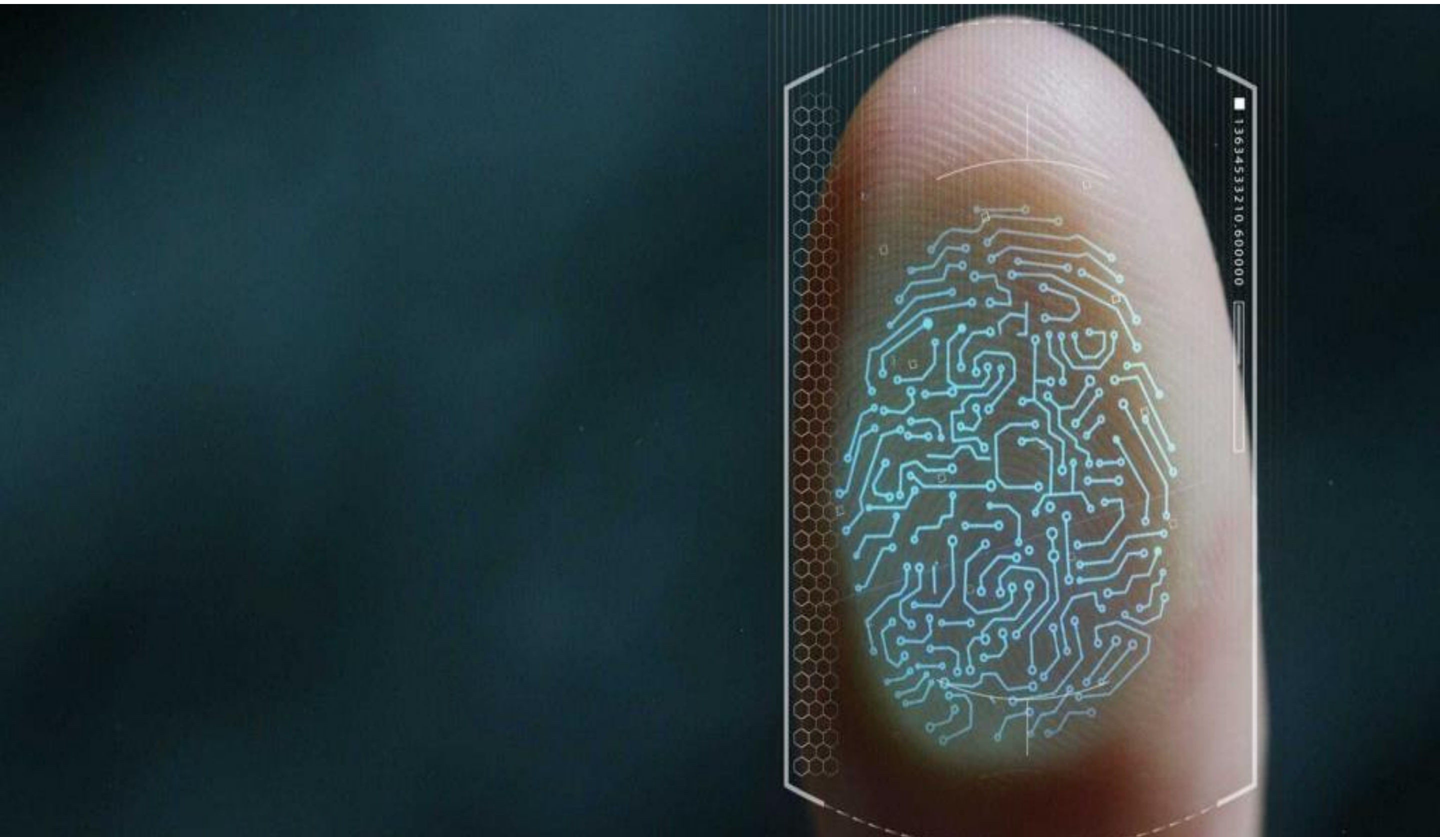
First Edition April 2020
© Goode Intelligence
All Rights Reserved

Published by:
Goode Intelligence

Sponsored by:
IDEX BIOMETRICS

Whilst information, advice or comment is believed to be correct at time of publication, the publisher cannot accept any responsibility for its completeness or accuracy. Accordingly, the publisher, author, or distributor shall not be liable to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by what is contained in or left out of this publication.

CONTENTS



THE GROWING ISSUE OF THE COST OF PAYMENT FRAUD

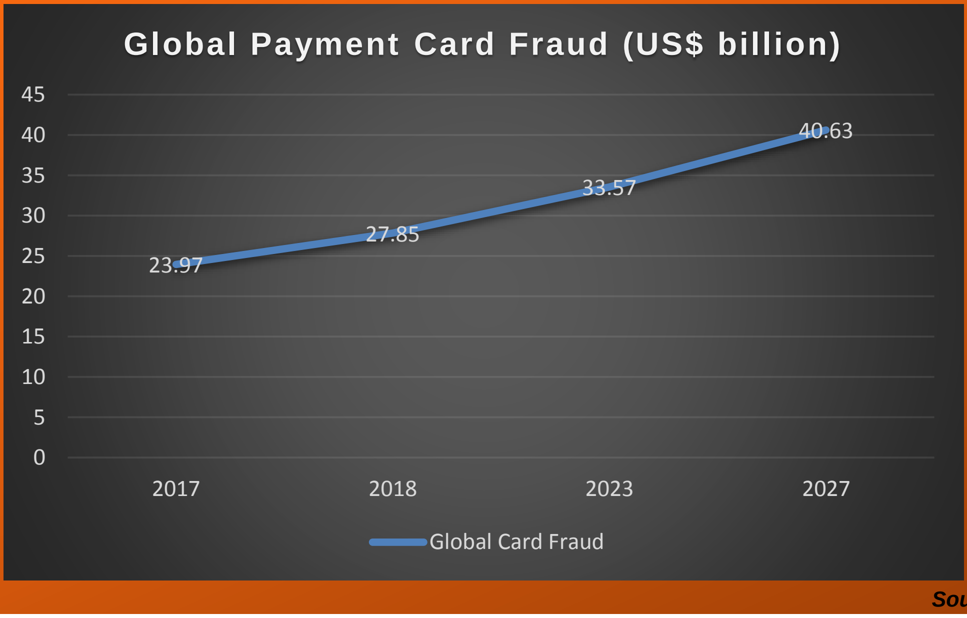
PAYMENT CARD FRAUD

A $28 BILLION GLOBAL PROBLEM

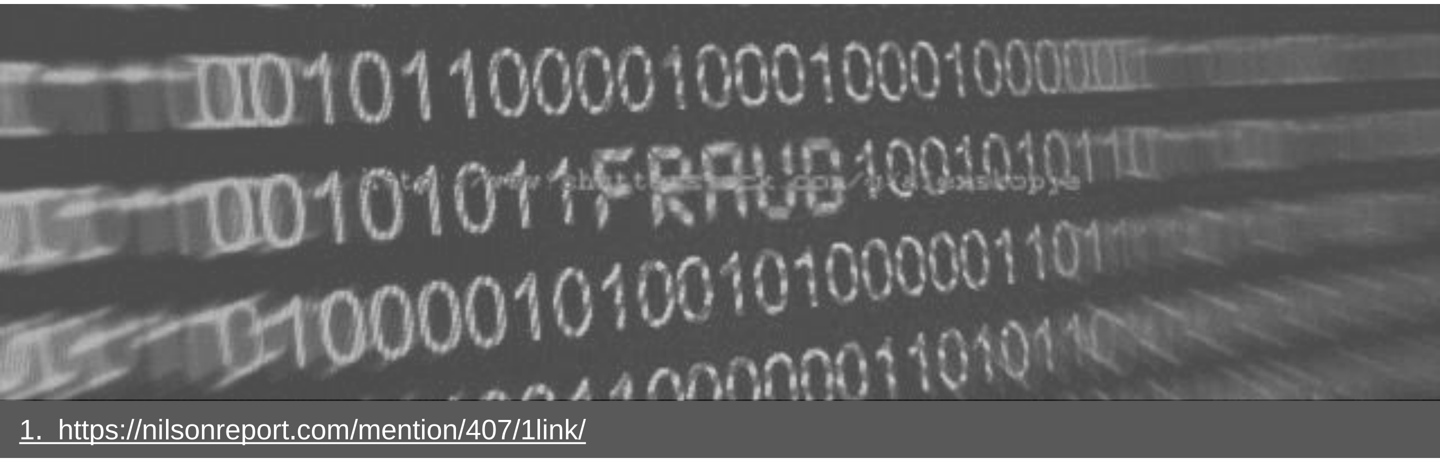
Global payment card fraud, both **Card Present (CP)** and **Card-Not-Present (CNP)**, is an ever-growing problem with billions of dollars of losses annually. Global card losses amounted to a staggering $27.85 billion during 2018 according to The Nilson Report. [1] This equates to 6.86 cents for every $100 total volume in 2018 and up on the figure of £23.97 billion recorded in 2017.

This is a problem that is not getting any better, with The Nilson Report predicting that global card fraud losses are set to rise to $33.57 billion by 2023 and $40.63 billion by 2027.

Chart 1: Global Payment Card Fraud



Source: The Nilson Report



[1] https://nilsonreport.com/mention/407/1link/

Card Present Use Cases

A transaction is described as being ‘card-present’ (CP) when the cardholder and the card are present at the same time. When the card that is presented is a chip card then it is placed in the terminal. Contactless card transactions are increasingly popular allowing a customer to touch a contactless card on a terminal. If a card does not have a chip, then the magnetic stripe on the reverse of the card is swiped through the terminal.

Card Present Examples

- Retail Point-Of-Sale (POS) systems with card readers (supporting both contact and contactless card transactions)
- Ticketing systems with card readers
- Car readers connected to smartphones or tablets

Card-Not-Present Use Cases

Globally, ‘card-not-present’ (CNP) fraud includes telephone, Internet, and mail-order telephone-order transactions where the cardholder does not physically present the card to the merchant.

Most CNP fraud involves the use of card details that have been obtained through skimming, hacking, email phishing campaigns, telephone solicitations or other methods. The card details are then used to facilitate fraudulent transactions. Although EMV deals effectively with counterfeit fraud, it does not address CNP fraud. With the migration to EMV for card-present transactions, fraudsters shift their focus to other channels, such as CNP transactions.

Card-Not-Present Examples

- eCommerce (online shopping carts)
- Recurring or subscription billing
- Electronic invoicing
- Mail Order Telephone Orders (MOTO)
- Payment apps on smart mobile devices

Card Fraud Methods

Card fraud is caused in four main ways, all connected with the attacker attempting to obtain either the physical card or card data, **lost or stolen cards**, **hacking** (including malware), **skimming** and **phishing**.

Lost or Stolen Cards

This fraud occurs when a fraudster uses either a lost or stolen card to make a purchase or a payment (both CP and CNP) or takes money out of an ATM. The card's PIN may also be obtained fraudulently through either coercion, shoulder-surfing, cameras installed on a compromised POS or ATM device or social engineering. In the UK losses from lost or stolen cards was £95.1 million in 2018 (a two percent increase from 2017). (2)

Skimming

This type of card fraud involves electronic copying of the data from the card which are then used for making counterfeit cards. Skimming occurs at perfectly legitimate transactions such as paying for goods or service at retailers such as restaurants where an unscrupulous employee puts the card into an electronic device to copy and save the key information but it can also occur at cash machines that have been fitted with tiny skimming devices. Victims of this type of card fraud are usually unaware of the problem until they check their bank balance showing transactions they didn't make.

Hacking

An attacker breaks into computer systems or places malware operated by the payment services industry, including retailers, restaurants, hotels, banks and payment services providers. With this stolen data, cybercrooks can produce cloned credit cards or commit other kinds of fraud, such as card-not-present fraud. They also can sell the data via underground marketplaces online.

Phishing

A phishing attack attempts to obtain sensitive card data by posing as a legitimate organization, such as a credit card company or bank, via email, phone or text (smishing).

2. Fraud The Facts, UK Finance.

Card Fraud in Europe

European Union

Fraud related to card payment schemes (CPSs) in the Single Euro Payments Area (SEPA), sourced from the European Central Bank's latest card fraud data, shows total fraud at €1.8 billion (approximately US$2 billion) in 2016. CNP fraud was the biggest contributor in 2016 with 73 percent of the value of card fraud. 19 percent was from transactions at point-of-sale (POS) terminals and 8 percent from transactions at automated teller machines (ATMs).

United Kingdom

In the United Kingdom, it has been estimated that £4.7 billion (approximately US$6.2 billion) has been stolen as a result of credit card fraud (3). The figure comes from a survey by Compare the Market (Credit Card Fraud Index) for 2018 that also found that on average, £801.00 (approximately US$1,050.00) is stolen for each person as part of the fraud. The two most common fraud methods were online (21 percent) and as a result of card skimming (11 percent).

Contactless card payments are becoming more popular especially in the European region. In the UK, contactless card payments accounted for more than 40 percent of all card transactions in 2018 and total UK contactless spend reached £69 billion (approximately US$90 million) over the course of the year, according to industry figures.

However, fraud on contactless payment cards accounted for more than half of debit and credit card crime during 2018, as fraudsters push the PIN-free limit, increased to £45.00 from £30.00 in March 2020 as a response to the Coronavirus emergency. Criminals are taking advantage of contactless payment cards to make as many purchases as possible, within bank limits on the number of repeated contactless transactions, before the card is blocked. Action Fraud, the national reporting centre for fraud and cybercrime run by the City of London Police, says that in the first 10 months of 2018, there were 2,739 reports of contactless fraud, totalling almost £1.8 million: up from 1,440 cases worth £711,000 (approximately US$924 million) in the same period in 2017. Average losses ran to between £90.00 and £625.00 with the largest single case resulted in a £400,000 loss, as a result of multiple purchases.

[3] https://www.paymentscardsandmobile.com/4-7-billion-stolen-from-uk-credit-card-fraud/

Card Fraud in Asia Pacific

According to FICO (4), CNP fraud is the most prevalent card fraud in the Asia Pacific region accounting for between 85 and 95 percent of all card fraud.

The overall trend is for increasing levels of CNP fraud as retail and payment moves online. For instance, in Australia CNP fraud accounts for almost 85 percent of the AUS$574 million (approximately US$386 million) total card fraud.

Card Fraud in the USA

The USA has become the go-to country for card fraudsters with the unenviable record of having the highest percentage of card fraud (by monetary levels) globally.

In the USA alone, card losses were $9.47 billion and accounted for 33.99 percent of gross card fraud losses worldwide.

In the USA, reports of credit card fraud has risen from 55,553 in 2014 to 157,688 reported cases in 2018.

The USA follows the rest of the world in seeing a significant rise in CNP fraud with customers 81 percent more likely to be a victim of CNP fraud versus card-present fraud. (5)

USA Card Losses

$9.47bn

33 percent of gross card fraud losses worldwide

4. https://www.fico.com/blogs/banking-fraud-what-s-happening-asia-pacific
5. https://shiftprocessing.com/credit-card-fraud-statistics/

THE GROWING ISSUE OF THE COST OF PAYMENT FRAUD

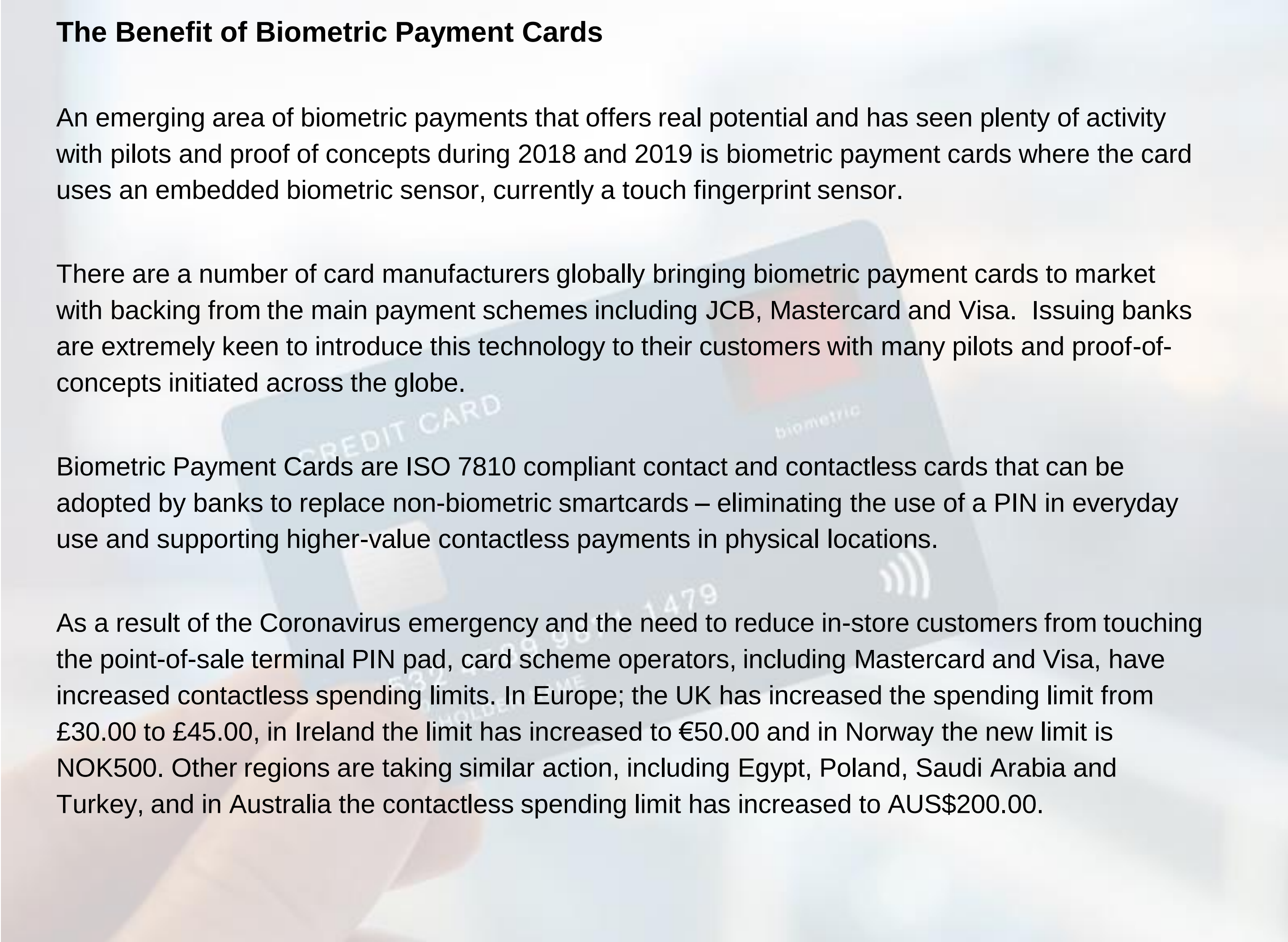
HOW BIOMETRIC TECHNOLOGY WILL REDUCE PAYMENT FRAUD

Biometrics – An Increasingly Important Technology in the Fight Against Fraud

Biometrics is an increasingly important technology in the fight against payment and card fraud and is being rapidly deployed to reduce both Card Present and Card Not Present fraud.

Biometrics has become an important tool in the fight against fraud in almost all payment channels. From cash obtained from ATMs to the newest ways of paying for goods and services biometric technology is being leveraged in traditional and emerging payment channels.

Biometric payment adoption is being driven by a number of factors that include a drive for **frictionless authentication** whilst paying in all channels, **industry and state regulation**, **a desire to reduce payment fraud**, and **technology standardisation**.



The Benefit of Biometric Payment Cards

An emerging area of biometric payments that offers real potential and has seen plenty of activity with pilots and proof of concepts during 2018 and 2019 is biometric payment cards where the card uses an embedded biometric sensor, currently a touch fingerprint sensor.

There are a number of card manufacturers globally bringing biometric payment cards to market with backing from the main payment schemes including JCB, Mastercard and Visa. Issuing banks are extremely keen to introduce this technology to their customers with many pilots and proof-of-concepts initiated across the globe.

Biometric Payment Cards are ISO 7810 compliant contact and contactless cards that can be adopted by banks to replace non-biometric smartcards – eliminating the use of a PIN in everyday use and supporting higher-value contactless payments in physical locations.

As a result of the Coronavirus emergency and the need to reduce in-store customers from touching the point-of-sale terminal PIN pad, card scheme operators, including Mastercard and Visa, have increased contactless spending limits. In Europe; the UK has increased the spending limit from £30.00 to £45.00, in Ireland the limit has increased to €50.00 and in Norway the new limit is NOK500. Other regions are taking similar action, including Egypt, Poland, Saudi Arabia and Turkey, and in Australia the contactless spending limit has increased to AUS$200.00.

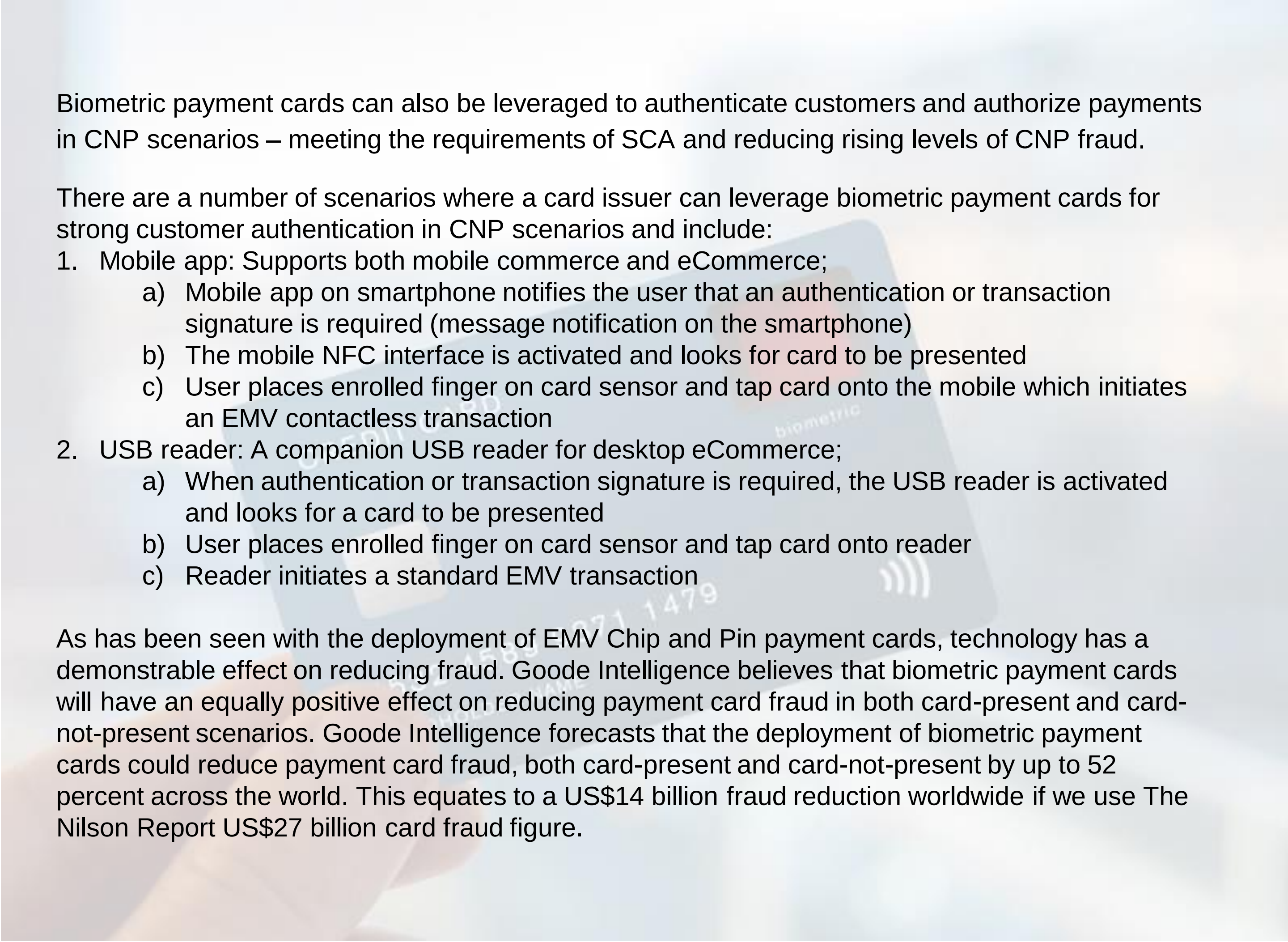
THE GROWING ISSUE OF THE COST OF PAYMENT FRAUD

HOW BIOMETRIC TECHNOLOGY WILL REDUCE PAYMENT FRAUD

The Benefit of Biometric Payment Cards

This action does not come without financial risk. A result of the contactless spending limit increase could be increasing levels of fraud. A way to mitigate both the risks of touching a shared PIN pad and increasing levels of fraud is a biometric payment card.

They operate in the same way as normal smartcards (in both contact and contactless modes) apart from the user having to present the card with enrolled finger on card sensor. There is a match between the person’s finger and a fingerprint template stored on the card. If the match is successful, the card does not request PIN or other CVM (Cardholder Verification Method). If the match is unsuccessful or not performed (no finger on sensor), then the card may ask for a PIN or decline the transaction.



Biometric payment cards can also be leveraged to authenticate customers and authorize payments in CNP scenarios – meeting the requirements of SCA and reducing rising levels of CNP fraud.

There are a number of scenarios where a card issuer can leverage biometric payment cards for strong customer authentication in CNP scenarios and include:

1. Mobile app: Supports both mobile commerce and eCommerce;
    a) Mobile app on smartphone notifies the user that an authentication or transaction signature is required (message notification on the smartphone)
    b) The mobile NFC interface is activated and looks for card to be presented
    c) User places enrolled finger on card sensor and tap card onto the mobile which initiates an EMV contactless transaction
2. USB reader: A companion USB reader for desktop eCommerce;
    a) When authentication or transaction signature is required, the USB reader is activated and looks for a card to be presented
    b) User places enrolled finger on card sensor and tap card onto reader
    c) Reader initiates a standard EMV transaction

As has been seen with the deployment of EMV Chip and Pin payment cards, technology has a demonstrable effect on reducing fraud. Goode Intelligence believes that biometric payment cards will have an equally positive effect on reducing payment card fraud in both card-present and card-not-present scenarios. Goode Intelligence forecasts that the deployment of biometric payment cards could reduce payment card fraud, both card-present and card-not-present by up to 52 percent across the world. This equates to a US$14 billion fraud reduction worldwide if we use The Nilson Report US$27 billion card fraud figure.

SUMMARY & NEXT STEPS

Payment card fraud is a $28 billion problem. Global payment card fraud, both Card Present and Card-Not-Present (CNP), is an ever-growing problem with billions of dollars of losses annually. Global card losses amounted to a staggering US$27.85 billion during 2018 according to The Nilson Report. This equates to 6.86 cents for every US$100 total volume in 2018 and up on the figure of US$23.97 billion recorded in 2017.

Payment card fraud is a $28bn problem

Goode Intelligence forecasts that by 2023, over 579 million biometric payment cards will be in use. (6)

Card fraud is caused in four main ways, all connected with the attacker attempting to obtain either the physical card or card data, **lost or stolen cards**, **hacking (including malware)**, **skimming** and **phishing**.

The good news is that technology does have an impact on reducing global card fraud. EMV, 3-D Secure, Tokenization, PSD2's SCA and Biometrics are crucial weapons in the fight against both Card Present and Card-Not-Present (CNP) fraud.

SCA is heavily influencing consumer authentication design and not only within the EU.

Built on the three principles of what you know, have and are, it is pushing biometrics into all aspects of consumer authentication for payments and is applicable for both card-present and card-not-present scenarios. A perfect example of this is the biometric payment card which, as we have demonstrated, is ideal for meeting SCA requirements in both physical and online retail settings and can lead to a **52 percent reduction in fraud costs**.

Next Steps

IDEX Biometrics would be delighted to demonstrate their fingerprint identification technologies which deliver simple, secure and personal authentication for all. If you are interested in exploring how your organisation could participate in a biometric smart card pilot then, in the first instance, drop an email to **sales@idexbiometrics.com**.

[6] https://www.goodeintelligence.com/report/biometrics-for-payments-market-technology-analysis-adoption-strategies-and-forecasts-2018-2023/

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consulting services for the biometric and authentication sectors.

We publish analyst and market intelligence reports, provide custom technology-driven market research and act as trusted advisors to our clients. For more information on this or any other research please visit www.goodeintelligence.com and follow @Goodeintel.

ABOUT IDEX BIOMETRICS

IDEX Biometrics ASA (OSE: IDEX and OTCQB: IDXAF) is a leading provider of fingerprint identification technologies offering simple, secure and personal authentication for all. We help people make payments, prove their identity, gain access to information, unlock devices or gain admittance to buildings with the touch of a finger. We invent, engineer, and commercialize these secure, yet incredibly user-friendly solutions. Our total addressable market represents a fast growing multi-billion-unit opportunity.

For more information, visit www.idexbiometrics.com and follow @IDEXBiometrics

6. https://www.goodeintelligence.com/report/biometrics-for-payments-market-technology-analysis-adoption-strategies-and-forecasts-2018-2023/