LEVERAGING YOUR PCI DSS INVESTMENT FOR GDPR

11th July 2018

datadivider

Leveraging your PCI DSS investment for GDPR

Table of content

Introduction

This white paper addresses how organizations who have implemented smart PCI DSS (Payment Card Industry Data Security Standard) programs can leverage their investment within their GDPR program. It starts by examining the potential impact PCI DSS is, and is not, having in addressing card payment fraud. It then takes a detailed dive reviewing fraud in the UK, where PCI DSS has been widely adopted, to attempt to analyse PCI DSS's impact. Next it measures this impact against other fraud detection efforts combating card losses once cardholder data has been breached. It then investigates where cardholder breaches are still being perpetrated to determine the effectiveness of PCI DSS in protecting card account data. Finally with this understanding the paper then looks at how the lessons learned within PCI DSS can be applied to GDPR in order to minimize an organization's cost and risks.

Global Fraud

Until 2016 global card fraud had been rising at alarming rates. In 2017 Nilson reported that card fraud worldwide had reached 7.15 cents per $100 totalling a massive $22.80B (see figure 1 – note 2016 published chart shows actuals until 2015 and estimates beyond this). However, the 2016 figure was $1.91B less than

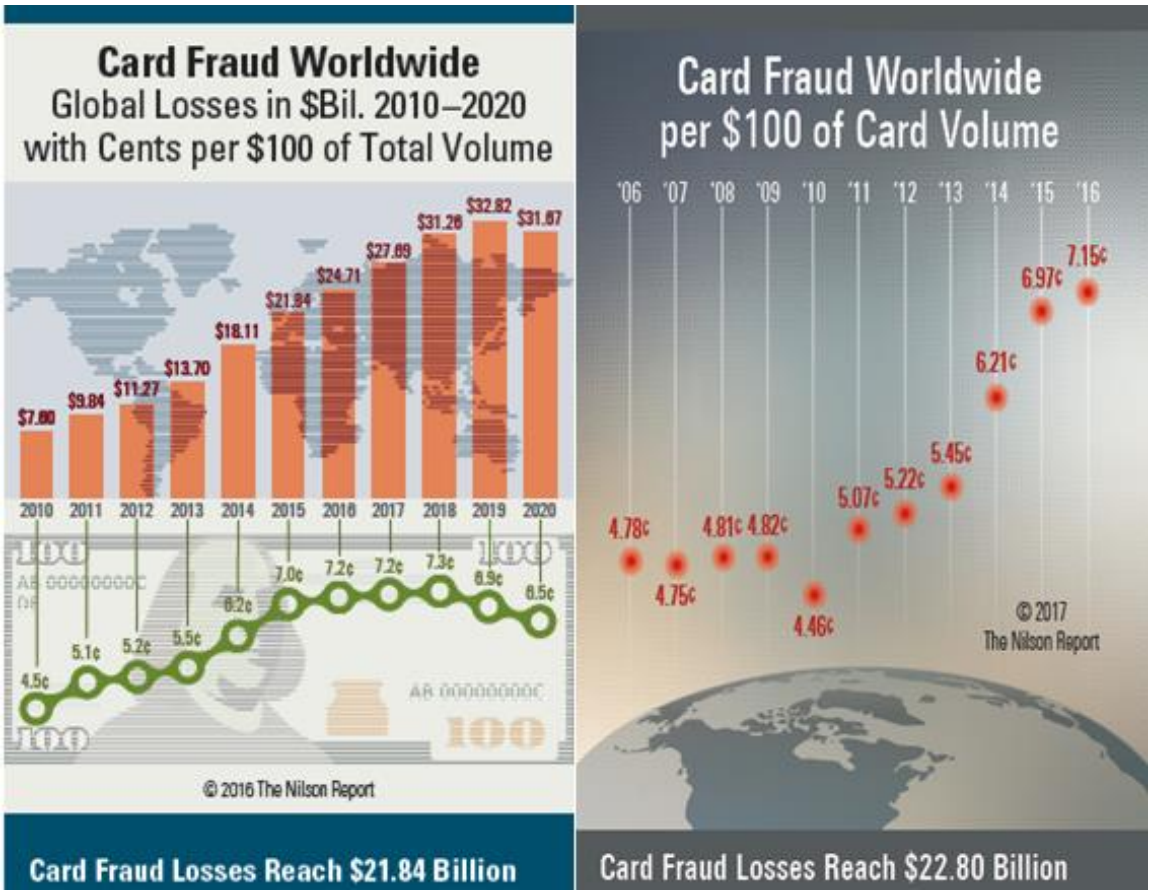


Figure 1: Worldwide Card Fraud - Source: Nilson Report Oct 2016 & Oct 2017

they had forecast the year before. So after an average annual growth in global card fraud of 23% in the previous five years growth in 2016 was just 1.1% growth. Not until October 2018, when 2017's numbers are published, will it be possible to see if global card fraud rates have truly levelled off. If so, this will be two to three years before Nilson, in 2016, forecast this declination.

UK fraud

Greater insight may be achieved in looking at UK card fraud where PCI DSS together with other fraud prevention techniques has been widely adopted. PCI DSS in the UK could be argued to be beginning to contribute to winning the battle in reducing credit card fraud as demonstrated by the annual reduction in 2017 of debit and credit card fraud from £618M to £566M[1] (see figures 2, 3 & 4). This 8.4% reduction was made up from a 15.7% in Card Present (CP) fraud and a 5.3% reduction in Card Not Present (CNP) fraud. While it is extremely positive that UK CP fraud is down by such a high percentage CP fraud accounts for only 27.7% of all card fraud. Also it is interesting to note that this 27.7% of fraud reduction is despite CP fraud cases in 2017 increasing by 24.0%. This represented a reduction of average CP fraud value from £485 to £330, a decrease of 32%.

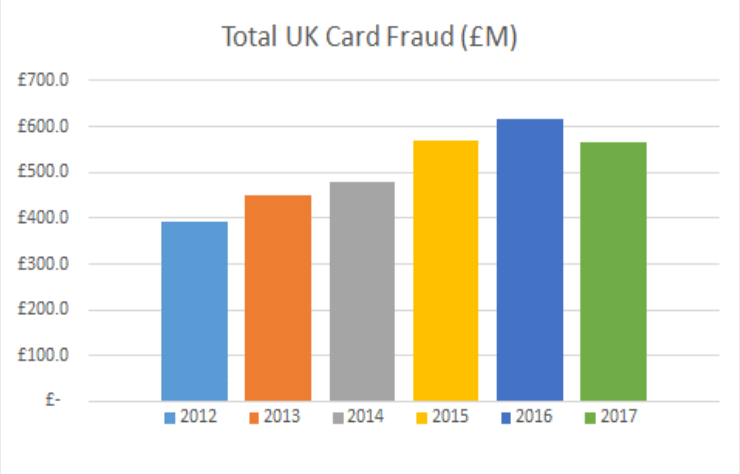


Figure 2: UK Card Fraud - Source: UK Finance 2017 annual update

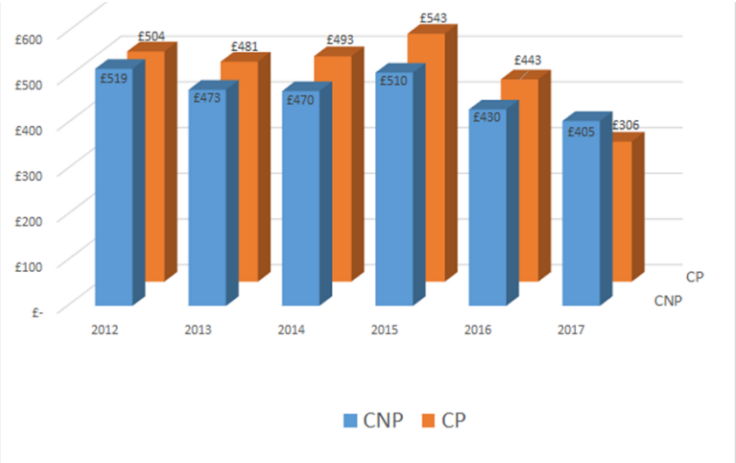


Figure 3: UK Average fraud value - Source UK Finance 2017 annual update

	2012	2013	2014	2015	2016	2017	16/17 %
Prevented value	N/A	N/A	N/A	£843.5M	£986.0M	£984.9M	0%
CP Losses	£143.1M	£149.1M	£147.5M	£169.9M	£185.8M	£156.7M	-15.7%
CNP Losses	£247.3M	£301.1M	£331.5M	£398.2M	£432.3M	£409.3M	-2.7%
Total losses	£390.4M	£450.2M	£479.0M	£568.1M	£618.1M	£566.0M	-8.4%
% Loss Change		15.3%	6.4%	18.6%	8.8%	-8.4%	
CP Cases	245,057	279,919	269,066	274,108	382,894	474,971	24.0%
CNP Cases	752,450	951,998	1,019,146	1,113,084	1,437,832	1,399,031	-2.7%
Total cases	997,507	1,231,917	1,288,212	1,387,192	1,820,726	1,874,002	2.9%
% Cases Change		23.5%	4.6%	7.7%	31.3%	2.9%	
CP Average Fraud Value	£ 584	£ 533	£ 548	£ 620	£ 485	£ 330	-32.0%
CNP Average Fraud Value	£ 329	£ 316	£ 325	£ 358	£ 301	£ 293	-2.7%
Average Card Fraud Value	£ 391	£ 365	£ 372	£ 410	£ 339	£ 302	-11.0%
Average Card Fraud Value Change		-6.6%	1.7%	10.1%	-17.1%	-11.0%	

Figure 4: UK CNP Fraud – Source: UK Finance 2017 annual update

[1] https://www.ukfinance.org.uk/wp-content/uploads/2017/06/UKFinance_2017-annual-fraud-update-FINAL.pdf

UK CNP Fraud – more analogous to GDPR

CNP UK Card Fraud	2012	2013	2014	2015	2016	2017	16/17 %
E-commerce	£140.2m	£190.1m	£219.1m	£261.5m	£310.3m	£310.2m	0.0%
Mail and telephone order	£107.1m	£111.0m	£112.4m	£136.7m	£122.0m	£99.1m	-18.8%

Figure5: UK Card Fraud - Source: UK Finance 2017 annual update

Diving even deeper it is interesting to note that all the reduction in CNP fraud was a result in reduced fraud rates in MOTO (Mail Order / Telephone Order) transactions (see figures 5 & 6). The UK mirrors the rest of the world where CNP fraud is the larger contributor to overall card fraud (see figure 7). CNP fraud is more analogous to GDPR breaches as there will not be P2PE (Point to Point Encryption) devices and chip based security to protect most personal data (most likely this will restricted to just credit and debit cards). Returning to the reduction in MOTO card fraud it should be noted that the UK pioneered both DTMF tone muting/masking and Data Capture Cloaking[2] in addressing telephone based payments. Both these techniques reduced the scope/footprint of cardholder data removing the opportunities for fraudsters to gain access to cardholder data. However, these technologies do not stop a fraudster from using perpetrated cards within call centres.

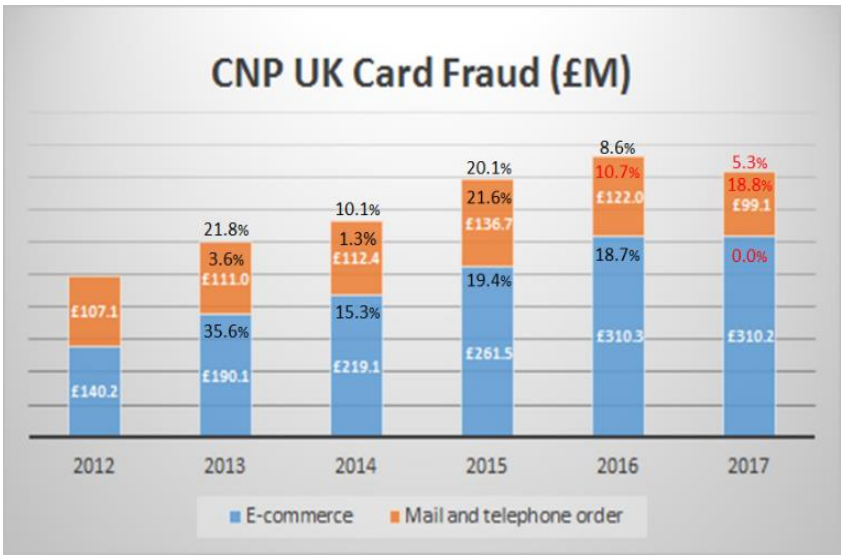


Figure6: UK Card Fraud Ecommerce & MOTO- Source: UK Finance 2017 annual report. Year on year increase/decrease shown as percentages

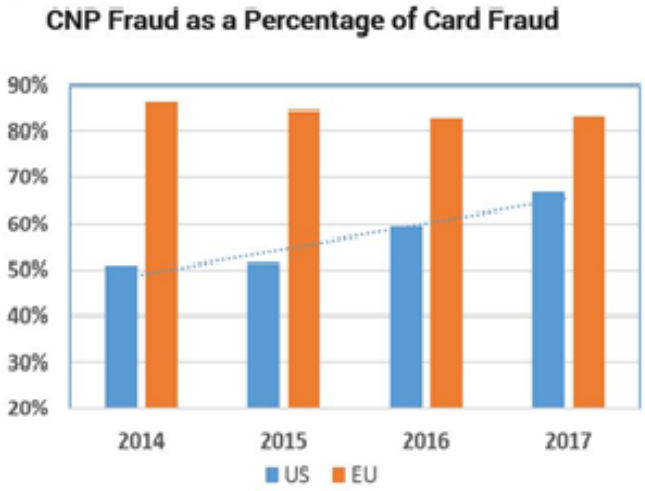


Figure7: US & EU CNP Fraud – Source: FICO Falcon Consortium

3DS for CNP Fraud

It is not yet possible to attribute the flat lining of UK Ecommerce fraud to the advances and increased adoption of 3D Secure 2.0 as this was still in its infancy of deployment in 2017. Many merchants are adopting 3D Secure (3DS) 2.0 because of the reduction in friction from utilizing additional cardholder data such as device information. Not only are 95% of issuers in the EU[3] now

[2] Data Capture Cloaking is a technique where by entered data is not exposed to the local device
[3] https://www.clearhaus.com/blog/3d-secure-and-3d-secure-2-0/

supporting 3DS 2.0 it is being claimed that cart abandonment rates have been reduced by 70%[4]. The advantage for merchants now is that they can attempt a 3DS transaction thereby shifting the fraud liability to the issuers yet for transactions failing 3DS they can accept or reject the transaction based on a fraud risk score.

With PSD2[5] (Payment Services Directive) forcing merchants in the EU to enforce Strong Customer Authentication (SCA) this might drive fraud to the rest of the world, however, this is not mandatory until September 2019[6]. It should be noted that 3DS 1.0 will cover PSD2 SCA, however, it is expected that most merchants will adopt 3DS 2.0 for more frictionless sales. Having fraudsters target non 3DS merchants, until this time in Europe and in the rest of the world, may reduce the average value of a fraudulent card transactions. Merchants with higher average baskets are more likely adopt 3DS 2.0. This is supported by the UK fraud card statistics where the average value of CNP fraud transactions decreased by 2.7% in 2017 (from £301 to £293). It is also interesting to note that this was further supported by the reduction of CNP fraud cases in the UK by 2.7% in the same period (see figure 2).

3DS 2.2 for MOTO

Having seen UK MOTO fraud reduce by 10.7% and 18.8% in 2016 and 2017 respectively 3DS could have further downward impacts to this fraud. 3DS 1.0 was not available for telephone based payments because only a static password was available. However, when 3DS 2.2 is made available it will include SCA for MOTO.

The UK government's Joint Fraud Task Force (JFT) is investigating the possibility of using 3DS 2.2 to tackle MOTO fraud on a voluntary basis for merchants[7] as PSD2 SCA does not cover MOTO transactions. Merchants will be able to challenge cardholders by the issuer providing a One Time Passcode (OTP) to the cardholder which can relayed back to the merchant and verified.

Domestic vs international fraud

A further piece of the UK card fraud statistics puzzle as it relates to the effectiveness of PCI DSS is where UK issued cards were compromised (see figures 8 & 9). In 2016 domestic card fraud only decreased 2.5%

Domestic /International split	2012	2013	2014	2015	2016	2017
UK fraud	£288.4M	£328.3M	£328.7M	£379.7M	£417.9M	£407.6M
UK fraud growth		13.8%	0.1%	15.5%	10.1%	-2.5%
Overseas	£102.0M	£122.0M	£150.3M	£188.4M	£200.2M	£158.4M
Overseas Growth		19.6%	23.2%	25.3%	6.3%	-20.9%

Figure 8: UK Domestic / International Card Fraud Split - Source UK Finance annual update

whereas overseas card fraud on UK issued cards decreased by 20.9%. On empirical evidence this could be associated with the adoption of EMV in the US. Historically the US has had a disproportionate amount of fraud as related to the cumulative value of US transactions (see figures 10 & 11). With adoption of chip based cards being processed by US merchants this is diminishing the opportunities of fraudsters skimming UK cards to perpetrate fraud in the US. So without the reduction of overseas perpetrated card fraud the 2017 8.4% reduction in UK card fraud would reduce to 1.7%. Therefore the effectiveness of PCI DSS and

[4] https://usa.visa.com/dam/VCOM/global/support-legal/documents/preventing-card-not-present-fraud.pdf (Slide 20)

[5] https://internationalbanker.com/banking/psd2-ready-strong-customer-authentication-sca/

[6] https://www.eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf

[7] https://www.cicm.com/wp-content/uploads/2018/02/CNP-MOTO-Industry-Consultation-V1.0Final.pdf

fraud prevention techniques in the UK in addressing UK card fraud can only be attributed to this smaller reduction.

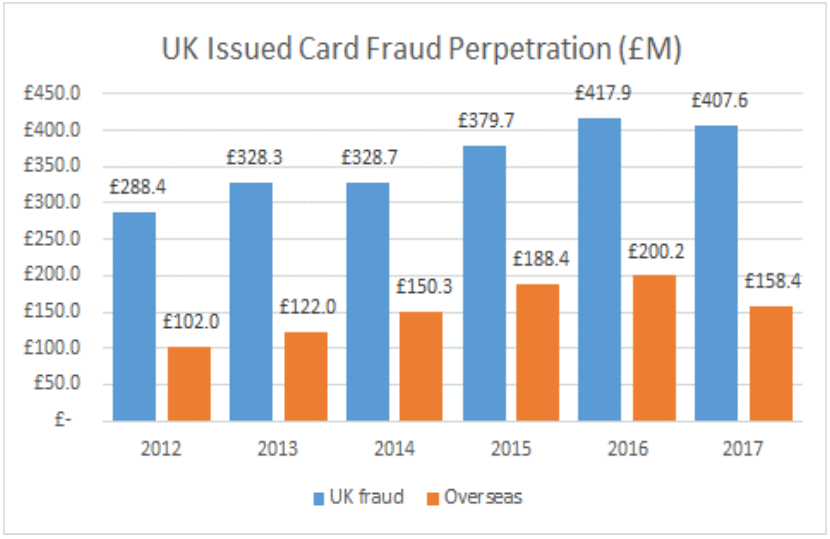


Figure 9: UK vs overseas fraud based on UK issued cards - Source: UK Finance annual report

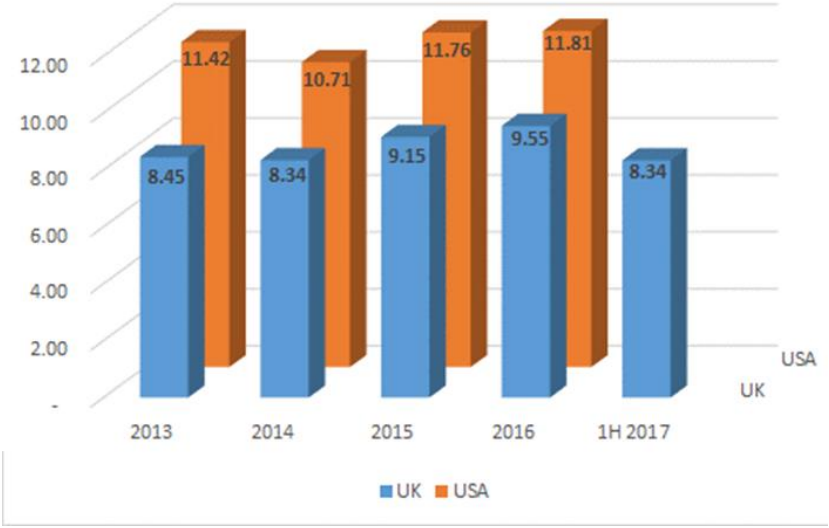


Figure 10: UK Finance 2017 annual report & Nilson Oct 2017 Report fraud cents per $100

Figure 11: Inside vs Outside the US Fraud cents per $100 – Source Nilson Report October 2017

PCI DSS forensic reports

The last piece of the UK card fraud puzzle worth examining is in the findings of forensic reports following PCI DSS breaches. Most PCI DSS breaches were perpetrated against businesses that were not PCI DSS compliant (see figure 12). It has been reported by some Qualified Security Assessors (QSA's) that there have been a small number of breaches involving internal actors where the merchant was PCI DSS compliant. So while the controls generate the necessary evidence of the fraud the data was nonetheless still stolen. It could be argued in these cases that the physical PCI DSS controls were not enforced but nonetheless organizations should be aware that protecting against internal actors for GDPR should be a priority. According to Verizon's 2018 Data Breach Investigations Report 27% of 2017 breaches were perpetrated by insiders. However, the overall conclusion from forensic investigations have been that PCI DSS as a set of security controls has been very successful in stopping fraudsters from gaining access to cardholder data.

TAKEAWAYS Unfortunately, 2016 showed some significant decreases in compliance levels when compared to previous years. None of the investigated breached merchants in 2016 were found to be compliant with PCI DSS. Furthermore, in nearly every case, the vulnerabilities attackers leveraged to gain access to merchant systems were covered by specific sections of the PCI DSS. In other words, had the organization been compliant with those sections of the PCI DSS, the breach likely would not have occurred.

Figure 12:`Takeaway from Security Metrics 2017 Guide to PCI DSS Compliance

PCI DSS vs fraud prevention reducing UK fraud

It is hard to conclude the reductions in UK card fraud are attributable to the wider adoption of PCI DSS within the UK. With the number of card fraud cases still increasing this could lead to the conclusion that a greater number of UK cards are still being breached. According to WorldPay, in each fraud case, there are between three and four fraudulent transactions per account[8]. Based on this data, and the assumption that UK fraud is being perpetrated based on UK issued cards, it would appear that over half a million UK cards which were compromised in 2017. It will be interesting to review the UK Finance 2018 annual update in early 2019 to see if the reductions in UK card fraud continues and if the wider adoption of PCI DSS across merchants, the greater adoption of 3DS 2.0 in the EU and the further adoption of EMV in the US are the most significant contributors.

PCI DSS effectively protecting card account data

Setting the impact to card fraud that PCI DSS maybe having globally and in the UK aside, the most significant fact that can be concluded is that organizations who have successfully implemented a PCI DSS program have ensured that they have been protected (especially against external fraudsters). The overriding conclusion here is that PCI DSS is very effective, if implemented correctly, in denying fraudsters opportunities to harvest cardholder data. This white paper therefore proposes that organizations adopt the lessons learned through PCI DSS in addressing the security requirements of personal data under GDPR.

Unlike PCI DSS GDPR is not a prescriptive regulation. It is clear that personal data should be made secure and it documents the potential fines should such personal data be compromised, however, it does not state how such data should be made secure. As the 300 plus PCI DSS prescriptive security controls have been successful in protecting card account data from outsiders it is proposed that these same controls be applied to securing GDPR personal data. Furthermore, as the PCI DSS controls have arguably been less successful in protecting cardholder data from internal actors it is proposed that this is additionally addressed in securing GDPR personal data.

[8] https://test.cunorthwest.com/wp-content/uploads/2018/04/WP-CUNW-SCCUA-1.pptx

GDPR Programs

Most organizations have initially focused their GDPR programs in identifying the personal data they manage, implementing the necessary opt in policies and providing with the necessary capabilities of personal data disclosure to meet their GDPR requirements. Whilst this is definitely necessary, unless this is coupled with implementing the security requirements for this personal data, the organization is leaving itself exposed to a potential GDPR breach. PCI DSS has been very poorly policed by the acquirers as they were being called upon, by the schemes (Visa, MasterCard, JCB, Discover and American Express), to sanction their customers. The moment that acquirers became aggressive in attempting to enforce PCI DSS merchants threatened to march with their feet to the acquirer's competitor. Acquirers therefore had to walk a tightrope of cajoling their merchants to embrace PCI DSS without driving their custom away.

GDPR has independent bodies throughout Europe enforcing its laws. Whilst these bodies, the Information Commissioner's Office (ICO) in the UK, may not necessarily have the resources in place to handle their new workload they certainly have the teeth that acquirers lacked for PCI DSS. With fines at their disposal of the greater of €20M or 4% of global revenue they will have businesses' attention. With major data breaches in the UK, post the 25th May 2018 GDPR enforcement date, already perpetrated at Dixons Carphone and Ticketmaster UK, all eyes will be on the ICO to see how quickly they react and what fines they enforce. This potentially will be the wakeup call that businesses need so that they do not rely on existing security controls to protect their personal data.

PCI DSS lesson learned

Having understood the necessity of protecting personal data for GDPR it is important to understand how to best leverage the PCI DSS investment for GDPR. There have been a number of key lessons learned in cost effectively achieving PCI DSS. The first of these has been how to de-value data. The primary techniques utilized within PCI DSS to achieve this have been through encryption and tokenization. It has also been discovered how critical it is to de-value the data at the endpoint at which the data is captured. Many frauds are perpetrated where data is being transmitted rather than at rest. If personal data is de-valued prior to transmission this eliminates this risk.

Tokenization rather than encryption

As tokenized data is deemed out of scope from PCI DSS controls there are considerable advantages of de-valuing data through tokenization. This eliminates the necessity of the 300 plus PCI DSS controls for the infrastructure handling tokens as opposed to cardholder data. The same principles will hold true for GDPR in that devalued personal data through tokenization is not at risk and therefore could be deemed out of scope for GDPR. By reducing the scope this can vastly reduce risk and the cost of securing personal data as less infrastructure requires the necessary security controls.

Most organizations have adopted third party token vaults. These have the advantage of protecting the personal data in certified cloud environments being protected by security companies. As the sole raison d'etre for these companies is to protect personal data their focus to this single pursuit ensures the highest levels of security. These companies are continuously penetration tested to ensure no security weaknesses ever enter their environment. Equally they ensure that personal data is only provided access from and to bonefide parties. Other organizations have implemented their own token vaults. They require all the same necessary security measures within their token vault area and however do not benefit from the economies of scale of independent token vault providers. It would be recommended that the PCI DSS controls be applied across the internal token vault infrastructure.

Point-2-Point Tokenization (P2PT©)

Where PCI DSS and GDPR diverge is that PCI DSS is predominantly concerned with numeric data and GDPR personal data is alphanumeric. So where endpoints have been secured with P2PE (Point to Point Encryption) devices for PCI DSS this will not be possible for GDPR. However, this does not eliminate the need to secure the personal data at the endpoint on which it is captured. By isolating the personal data from the endpoint device and performing tokenization within this isolated environment it is possible for the end device to only be exposed to de-valued data. This isolation is achieved by creating a secure environment on the device with remote security controls that shield it from the device itself. These protections afford the ability to still secure the personal data even if the device itself has been compromised. So for GDPR it is recommended Point to Point Tokenization (P2PT)© is adopted to achieve the same level of security as P2PE achieved for PCI DSS. Having established this secure isolated environment on the device then the device can be securely connected with an audit certified cloud where tokenization and communications to third parties can be managed. This secure cloud environment provides remote sessions on which the personal data is captured and visualized to the endpoint device. As the isolated environment on the device prevents any keyboard logging, screen printing and frame images the personal data remains secure. In effect the remote session visualized on the protected endpoint device just uses the device for the secure capture of keystrokes. The actual personal data is captured within the remote session running in the secure cloud. This eliminates the opportunity for a fraudster to gain access to the personal data even if they have compromised the endpoint device (see figure 13[9]).

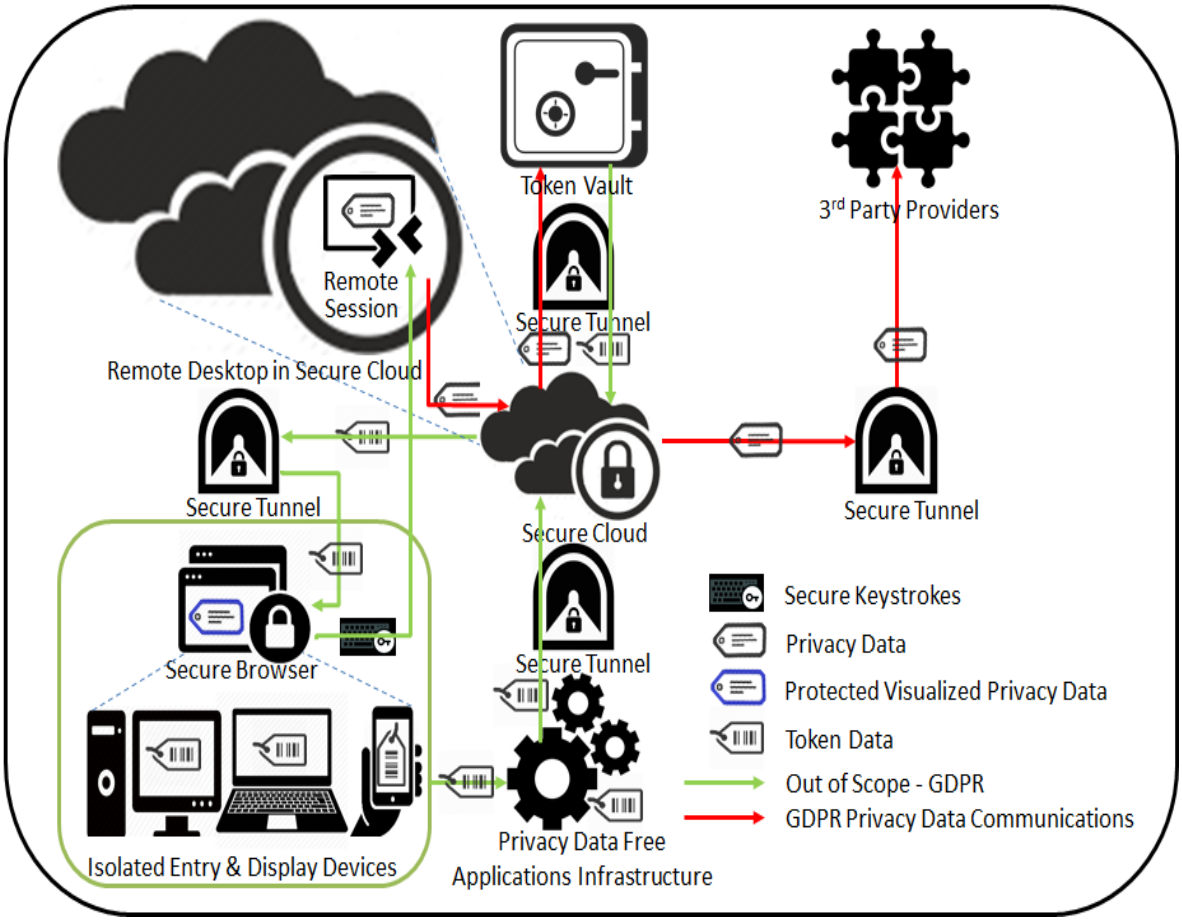
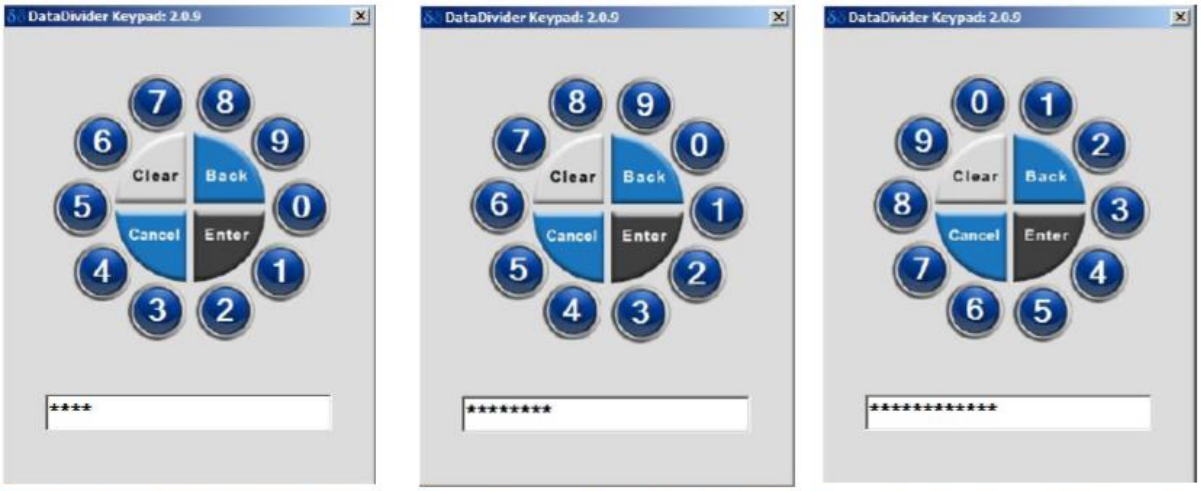


Figure 13: Devalued Personal data GDPR Architecture for contact centre and back office data capture

[9] DataDivider Patent Pending

Isolating and protecting numeric data

With PCI DSS, which secures numeric data, it was possible to protect endpoint devices against hardware keyboard loggers with Data Capture Cloaking. Data Capture Cloaking utilizes mouse clicks for data entry. By randomizing the location of digits and protecting frame images it is not possible to correlate a mouse click coordinate with a digit in the cardholder data (see figure 14). Whilst this can be extended for the entry of alphanumeric strings, such as the UK National Insurance (NI) number, it is impractical for general data input.



The Virtual Keypad initiates with the digit zero being randomly placed between 1° and 360°. Following the mouse click entry each digit is masked. From the first 2 digits it is possible to determine the card format, 4-4-4-4 for MC and Visa, 4-6-5 for Amex and 4-6-4 for Diners Club.

Following the entry of each cluster of digits the Virtual Keypad rotates 1 or 2 digits clockwise or counter-clockwise. Most cardholders read their card number in clusters of digits following the card format. This makes entry simple for the call center agent.

Through the Virtual Keypad initiation and its rotation after each cluster of digits it is not possible to associate mouse clicks with card number digits. It is therefore impossible to reverse engineer mouse clicks back to the cardholder data.

Figure 14: Data Capture Cloaking utilized to collect cardholder data for PCI DSS

Isolating and protecting alphanumeric data

In these cases the physical keyboard will be required for capturing personal data into the remote session. The secure browser protects this data entry from software keyboard loggers, however, physical keyboard loggers could intercept this personal data. It is therefore necessary to have security policies that protect against hardware keyboard loggers. These should include machine inspections and preventative measures to stop software harvesting from such devices. Hardware keyboard logger perpetrated frauds are rare as they require physical access to the machine and unless the keyboard logger can attach to a wireless network they require that same physical access to harvest the captured data. To guard against wireless network based hardware keyboard loggers wireless networking monitoring should be implemented to detect non-authorized networks. Most hardware keyboard logger perpetrated frauds have been in public building such as libraries where it is difficult to implement secure access controls. It is possible to eliminate this risk by deploying specialist hardware which not only secures the physical USB port but can detect the presence of a hardware keyboard logger. The USB port is secured by an adaptor that locks the USB port (see figure 15). Any attempt to remove the device renders the USB port as unusable. The USB lock adaptor

Figure 15: USB Filter and USB locks

is then connected with a custom keyboard. The adaptor is able to detect if any hardware keyboard logger is between itself and the custom keyboard. In order to ensure that this security is not bypassed further hardware can lock the remaining USB ports.

Having isolated and protected devices significantly reduces the complexity of securing GDPR personal data. As the isolated protected device communicates directly with the token vault no personal data is exposed to the organization's infrastructure. In effect, the organization has de-scoped GDPR personal data to just the token provider and the isolated protected device provider.

Need to know for GDPR

Many applications today display personal data to an employee of an organization when there is no requirement for this personal data to be known for the employee to carry out their function. Although the secure browser can protect this personal data it should be questioned why this data is being exposed to the employee themselves. Certain personal data will be required for authenticating the customer but this should be limited. Today this is often date of birth and Post Code together with 1st line of address. This is personal data that is valuable to a fraudster. Other data which has much lower value could be used for authentication such as just day and month of birth, last four digits of mobile phone number on file and last four digits of bank account number on file. By using partial information this de-values the personal data and avoids the necessity of sharing all the personal data with the employee. Other examples which could be used for authentication include sort code/routing code of bank on file, mother's maiden name, last three digits of Social Security Code/last three characters of NI number and digits from post code. Superfluous personal data should not be shared on user screens where this information is not required.

Communication of personal data with 3rd parties

The management of personal data within the business where personal data is required for more than viewing on a device still needs to be addressed. Where the personal data is required to communicate with bonefide third parties then this can be managed through the secure cloud environment again not increasing GDPR scope or exposing the organization to personal data. Communications with the third party can be via the secure cloud provider where detokenization can take place. To further ensure that the third party also securely manages this personal data it is possible for the third party to also use the secure cloud's tokenization service. If the third party is managing personal data for multiple clients it has the option to use its own tokenization policy. In this case the secure cloud can act as a tokenization broker[9] where prior to sending personal data it would detokenize based on the client token policy and then tokenize based on the third party token policy. The third party can ensure that only when needing access to the personal data that de-tokenization takes place.

Where personal data must be printed for external distribution then it would be recommended to utilize a specialist secure partner. If printing is required internally then an isolated network would need to be established with all PCI DSS security controls applied within this environment.

Part of the PCI journey included the removal of cardholder details from all media. For example all cardholder numbers were replaced with just showing the last four digits of the card. Organizations need to do likewise with media on which personal data is shared which is not necessary for the communications itself.

Communication personal data with customers

Where personal data is to be shared electronically with the customer themselves then this can be engineered in a manner again not exposing this personal data within the business itself. Where customer details are being accessed by the customer through the internet the iFrame serving the customer can be rendered from within the secure cloud itself (see figure 16[9]). The content of the web page can be provided

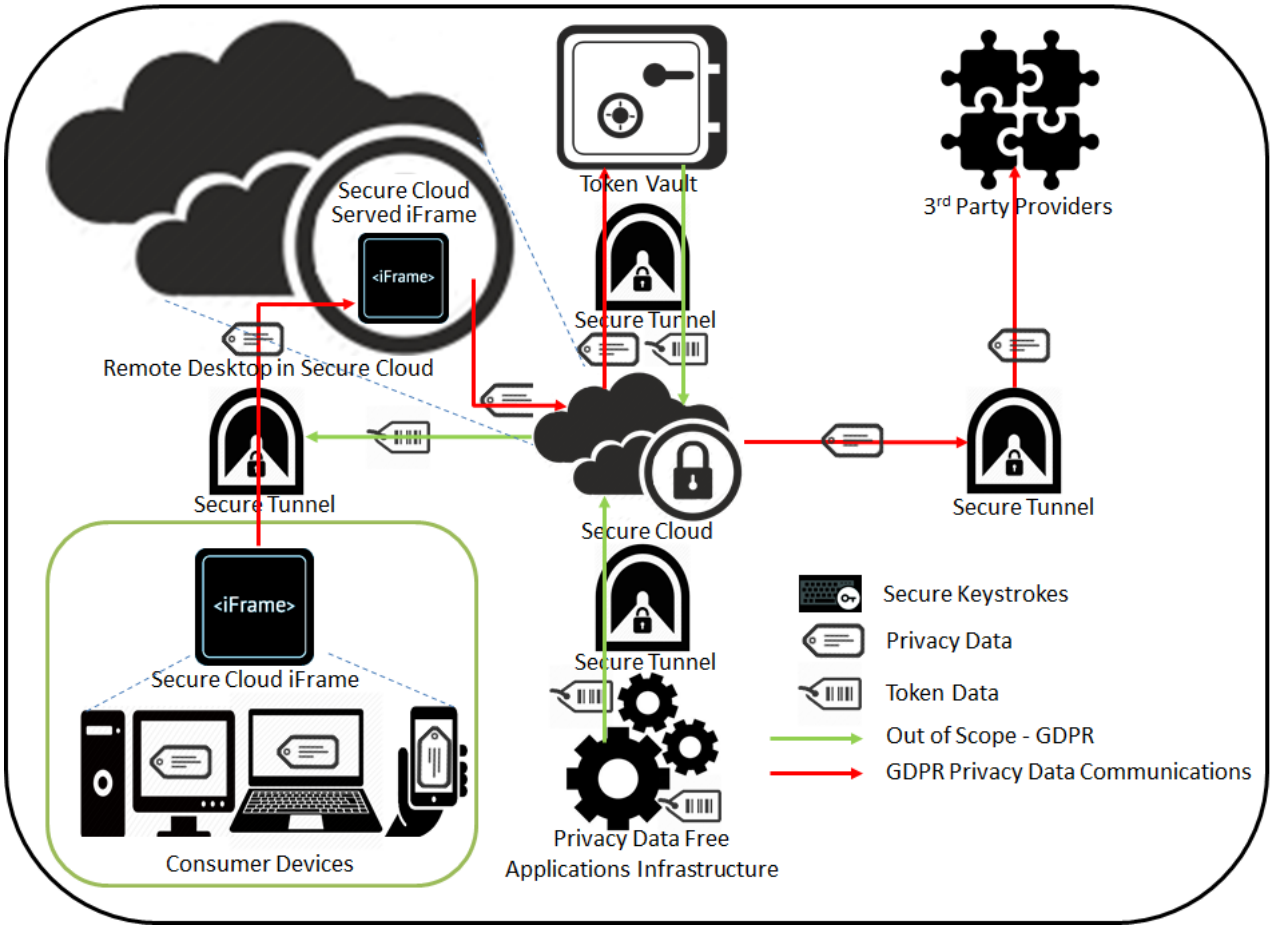


Figure16: Devalued Personal data GDPR Architecture for Internet data capture & data presentation

by the businesses' application where the personal data is represented within tokens. The secure cloud can then de-tokenize prior to sharing the privacy information with the customer. The reverse also needs to be true where customers are initially creating personal data. By serving the iFrame from the secure cloud all personal data can be tokenized prior to sharing this data with the business applications. This is the role that was provided by Payment Service Providers (PSPs) for PCI DSS ensuring that merchants were not exposed to cardholder data prior to the tokenization process.

Businesses also receive personal data by other mediums. Email, fax and mail all need to be covered. Fax and post can be scanned and then images can be OCR (Optical Character Recognition) read. Recognized personal data can then be tokenized and the scanned images updated to replace the personal data with tokens. The business can then process the communications but rather than adding the native personal data they can enter the tokens. The same process is a little simpler for emails as they can be electronically scanned for personal data within the secure cloud and then this data can be replaced with tokens.

Secure outbound calling

For businesses with outbound calling it is possible for employees to call customers without exposing these staff and applications to clients' phone numbers. By hosting outbound dialling at a third party or within the

secure cloud itself it is possible to make the requested call based on the telephone number token. As this request is processed by the secure cloud the actual telephone number is derived through the de-tokenization process. This can then be used for dialling or passing onto the secure 3rd party outbound calling providers.

Fox in the hen house

Finally organizations need to address how to protect GDPR personal data from internal actors. A small number of merchants, who did not implement the necessary physical controls, were breached when PCI DSS compliant. De-valuing the data through tokenization achieves the first step in protecting this personal data. The next required step is in controlling bulk detokenization. Only a few bonefide processes will require this function. By restricting bulk de-tokenization to these bonefide processes and alerting upon bulk de-tokenization it is possible to safe guard against fraudulent internal actors. Monitoring of these processes is essential such that alerts can be set off before the breached data is able to depart electronically or physically.

Conclusions

In conclusion, organizations that failed to become PCI DSS compliant were at risk of a breach at any time. Those that have achieved PCI DSS compliance protected themselves against card account breaches. In order to protect themselves against GDPR breaches they will have to extend their PCI DSS programs to include all personal data. GDPR programs need to quickly evolve from supporting the mechanics of managing personal data to protecting this data. The benefit from many of the gains achieved within PCI DSS can be applied for GDPR. The key to most successful PCI DSS programs was the devaluing of data and reducing the scope of where it was necessary to protect card account data. PCI DSS compliance was feasible with encryption but this did not reduce the scope and therefore did not reduce the cost. Tokenization on the other hand not only devalued the data it also reduced the scope. By tokenizing within iframes merchants got the best of all worlds by not being exposed to cardholder data. This was replicated for call centres through DTMF tone masking and Data Capture Cloaking. By adopting these same tokenization strategies for all GDPR personal data and implementing the tokenization and de-tokenization within isolated secure devices/environments it is possible to vastly reduce the cost of GDPR and the risk of GDPR breaches.