consult hyperion

securing tomorrow's transactions

GDPR: Banks, Breaches and Billion Euro Fines

Are Financial Institutions Ready for the 72-hour Notification Challenge?

Consult Hyperion, June 2017
Commissioned by AllClear ID

AllClear ID

Table of Contents

Executive Summary

The European Union's new General Data Protection Regulation (GDPR) introduces 72-hour breach notification requirements along with severe regulatory fines and consumers and affected third parties now have the right to sue organisations responsible for data breaches. Most financial institutions are focusing on prevention—as they should—but the highest risk item in the GDPR is the breach notification requirement, and banks are not mitigating this.

The highest risk item in the GDPR is the 72-hour breach notification requirement.

The chances of a breach occurring are increasing due to the conflicting requirements of new European financial service regulations. The ePrivacy Regulation, the Anti-Money Laundering Directives and the Second Payment Services Directive simultaneously increase the scope and longevity of personal data while mandating the introduction of new channels that allow third-parties to access some of it.

Based on an in-depth analysis of historical breach data, we conservatively forecast that European banks can expect fines in the region of €4,662 million in the first three years after the introduction of GDPR. These figures do not include compensation claims, costs associated with lost customers, damaged reputations and senior executive resignations.

These Fines Are Not Inevitable

GDPR requires the regulators to take into account the planning and mitigation strategies that a breached organisation implements. Effective planning can ensure that customer concerns and harm are dealt with promptly, and that the value of the data compromised is degraded. Proper breach response programs forecast the deluge of customer communications an institution will face after a breach and provision the required expertise, infrastructure and manpower to respond at scale in a matter of hours. The program should minimise the risk of identity theft, customer loss, reputational damage and reduce the possibility of consequential compensation claims.

European banks can expect fines in the region of €4,662 million in the first three years after the introduction of GDPR.

However, all of this relies on executives recognising that prevention alone is not sufficient to manage the risks associated with GDPR. Resilience is equally important.

Proper planning is the equivalent of household fire insurance—householders may take fireproofing measures to protect their homes, but the sensible ones ensure they have proper insurance coverage as well. In both cases the equation is the same—the risk may be small but if the worst should occur the consequences for the unprepared are huge.

This paper lays out the detailed challenges that GDPR poses for financial institutions, analyses the potential regulatory costs and identifies the measures that need to be taken to mitigate any actual breach. Critically banks must have:

- contingency plans in place to rapidly notify their entire customer base
- trained manpower to handle the deluge of customer queries
- secure communications infrastructure pre-deployed to safeguard customer interactions
- post-breach identity solutions ready to handle the ongoing customer issues

With only 72-hours to mobilise, financial institutions that do not plan ahead are certain to face serious GDPR fines, executive loss and collateral business damage. In other words, those that fail to plan are those that are planning to fail.

Introduction

Data breaches are an unfortunate fact of life for financial institutions. Interacting with suppliers and customers means that organisational boundaries are permeable and open up systems for fraudsters to gain access to customer data. Although companies should build the best defences against these, it is inevitable that breaches will occur.

A data breach can already cost senior executives their jobs and have serious reputational, brand and business impacts. Under GDPR the financial penalties could be catastrophic. Institutions can receive fines of up to 2% of the previous year's annual revenues for a first offence and 4% for repeat offences where the regulator has previously ordered remedial action. There are also possible criminal penalties for executives deemed responsible[1], and consumers and affected third parties now have the right to sue organisations responsible for data breaches.

A brief look at the statistics for data breaches in the financial sector shows why executives should be worried.

Globally, between 2013 and 2016 there were over 3000 reported data breaches in the financial sector of which over 40% led to proven data loss. In the absence of the mandatory reporting that GDPR requires these numbers are almost certainly understating the problem.

Resilience, Not Just Prevention

Prevention may be the best policy, but it is unlikely to be a universally successful approach.

Under GDPR's 72-hour breach notification requirement, they need to plan and manage data breaches in an open and effective manner becomes even more important. Regulators have significant discretion in the level of penalties they can levy, and are required to take planning, notification and mitigation into account in the decision[2]. Failing to properly care for customers affected by a data breach will severely limit regulator discretion.

Companies that have dealt with data breaches poorly have seen loss of customers, reduced earnings and board level resignations, while those with a prepared plan and a managed response have sidestepped these issues.

---

[1]For instance, the new German Federal Data Protection Act can lead to up to three years in prison for managers and data protection officers."

[2]As stated in rationale 148 of GDPR:

> "Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor"

Target v Home Depot

The US retail chains Home Depot and Target both suffered serious data breaches, but the results of these in terms of executive loss and quarterly earnings could hardly be more different. The quality of the response to a breach makes a huge difference.

	Target	Home Depot
Population Affected	40 million	56 million
Time to Notify	Weeks	Days
Quality of Response	Low	High
Δ in US Same Store Sales (QoQ%)	-0.4%	+5.8%
Δ in Quarterly Earnings	-46%	+14%
Stock Price	-11.9%	+ 4.3%
	12.31.13–2.28.14	9.1.14–10.31.14
Executive Loss	CEO + CIO	None

Target's quarterly earnings dropped 46% and its CEO and CIO resigned, while Home Depot's earnings actually increased, and they suffered no executive losses.

Proper preparation requires planning to ensure the right expertise, manpower and infrastructure is in place to deal with the issues when they occur. With only 72-hours to react, financial institutions that have not planned ahead are certain to face serious fines, lawsuits and collateral business damage.

The public reporting of breaches, as required under GDPR, triggers waves of customer calls. Institutions that rely on their own general purpose in-house customer services teams will find them overwhelmed by the volume and nature of the customer calls—leading to loss of customers, bad media coverage and ultimately the loss of senior executives.

The quality of the response to a breach makes a huge difference.

Target's quarterly earnings dropped 46% and its CEO and CIO resigned, while Home Depot's earnings actually increased, and they suffered no executive losses.

Speed and Quality Determine the Outcome

Ultimately the effectiveness of a breach response will be determined by two factors: speed of the notification and quality of the response. The chart below demonstrates how only a rapid response of the highest quality will result in a successful response.

Speed Criteria
of hours to notify DPAs
of hours to notify customers

Quality Criteria
Customer Response Preparation
Crisis Decision Making
Outbound Communications
Inbound Communications
Average Answer Times
Excalation Handling
Fraud & Identity Repair
Customer Satisfaction & Retention

Speed of Notification is measured by the number of hours from becoming aware of the breach until regulators are notified (no longer than 72-hours under GDPR) and the number of hours until customers are notified (without undue delay under GDPR).

The Quality of the Response is measured by the level of documentation and practice behind the customer response plan, the quality of executive decision making during the crisis, effectiveness of the outbound customer communication, customer service levels on the inbound communications including average call and email answer times, escalation handling, fraud and identity repair and overall customer satisfaction and retention.

A Regulatory Cocktail

To exacerbate the issue a number of other European regulations are coming into force in similar timeframes:

- The Second Payment Services Directive (PSD2) forces financial institutions to open up access to account data to third-parties
- ePrivacy Regulation (ePR) widens the scope of electronic communications data that qualifies as personal data
- Anti-money laundering directives AMLD4 and AMLD5 require the capture and storage of ever more personal data

At the point at which losing personal data becomes an expensive proposition for financial institutions they are simultaneously being regulated to hold more of it and make some of it available over open interfaces.

The financial penalties under GDPR may serve to focus minds on the issues surrounding data protection, but badly managed data breaches can have other, even longer term, effects.

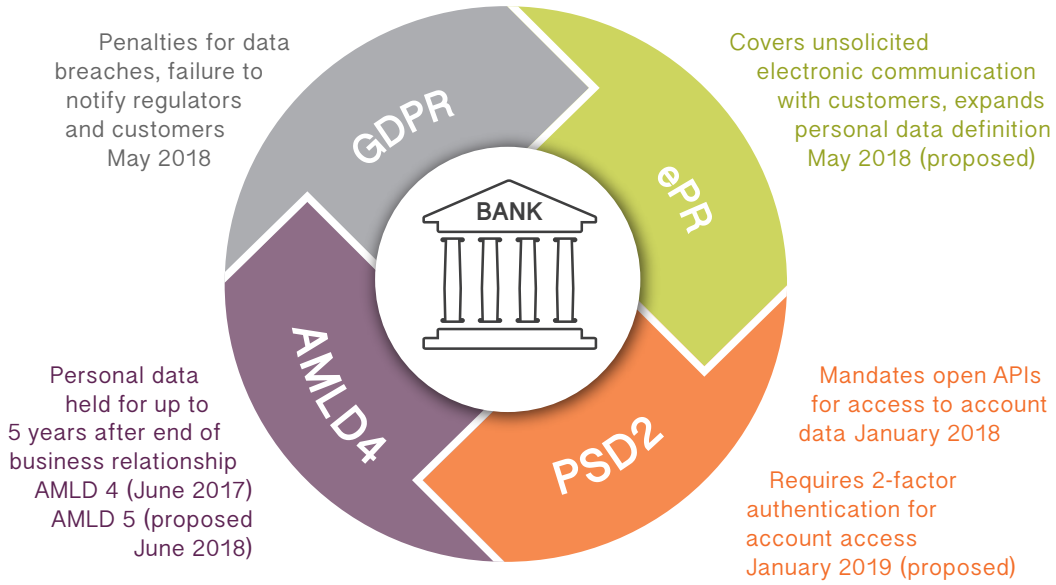
This white paper analyses the potential impact of GDPR on European financial institutions, forecasts the cost of data breaches and examines how both regulations and the impact of digital transformation compound these issues. Finally, it identifies the strategic considerations for the impacted institutions and offers practical advice on how to deal with these.

A Vicious Circle of Regulation

GDPR introduces a range of new regulations that includes mandatory reporting of data breaches to both regulators and customers and the potential for fines of between 2% and 4% of the previous year's annual turnover.

Compounding the GDPR issue for financial institutions are a range of other new European regulations—ePR, AMLD4 and AMLD5, and PSD2. Each of these individually creates a compliance headache, and combined they constitute a minefield as complying with one regulation exposes potential liabilities under the others:

- GDPR imposes 72-hour notification and mitigation requirements on data breaches
- ePR extends the definition of personal data to cover anything that can be used to contact a customer
- PSD2 requires that banks open up APIs to allow third-parties to access customer data with the appropriate consent of the customer—using two factor authentication—and potentially exposes legacy core banking systems via new digital channels
- AMLD4 and AMLD5 requires additional customer data to be stored and held for up to five years after any business relationship has ended



Takeaway—Banks must hold more data, open up access to some of it and face penalties for a data breach

IN SUMMARY

AMLD4/5 increases the scope of customer data to be stored, PSD2 provides new channels to allow third-parties access to some of these data, and GDPR/ePR widens the scope of personal data and impose severe fines if any of these data is exposed without consent.

This vicious circle of regulation creates a huge headache for financial institutions by increasing the risk surface for attacks and amount of data held, while simultaneously introducing enormous penalties for data breaches.

Takeaway: Banks must hold more data, open up access to some of it and face penalties for a data breach

The Cost of GDPR for Financial Institutions

The record of data breach reporting in the financial sector is patchy, with little mandatory reporting in the EU, but based on the available data[3] globally there were on average 514 verified breaches per year in the financial sector between 2013 and 2016.

With a quarter of the world's banks in the European Union and no discernible difference in the regional pattern of reported breaches this implies there are around 128 breaches in the financial services industry each year in the EU. This is a highly conservative estimate.

Analysis suggests that there have been no fewer than 27 data breach incidents among Tier 1 banks in the last decade, with some banks as multiple offenders, potentially liable for fines at the 4% level. This indicates an 8% chance that any Tier 1 bank will suffer a data breach in any given year.

We expect see 2–3 breaches of Tier 1 banks, six breaches of Tier 2 banks and a long tail of breaches in Tier 3 financial institutions over three years. We estimate the average Tier 1 bank fine will be €260 million and the average Tier 2 bank fine at €48 million. These figures do not include compensation claims, costs associated with lost customers, damaged reputations and senior executive resignations.

Our conservative analysis forecasts that European banks can expect fines in the region of €4,662 million in the first three years after the introduction of GDPR.

Our conservative analysis forecasts that European banks can expect fines in the region of €4,662 million in the first three years after the introduction of GDPR.

Data breach forecast and costs

Type of bank	Total number of banks	Forecast average fine (millions)	Forecast breaches	Estimated fines (millions)
Tier 1	32	€260[4]	2/3	€666
Tier 2	75	€48[5]	6	€288
Tier 3	5000	€5[6]	120	€600
Total Year 1 = €1,554				
Total Over Three Years = €4,662				

These figures, we believe, are conservative. Historical data almost certainly underreports the true level of bank breaches. An additional breach by a single large Tier 1 bank or fines at the higher 4% level for failures to meet remedial corrective orders from the regulators could see these figures rise significantly.

It should also be noted that under GDPR Article 82 any person suffering damage as a result of a data breach has the right to compensation at a level determined by the law of the Member State where the infringement occurred. Similarly, a third-party organisation that suffers losses as a result of the data breach can also claim compensation. This compensation may cover administrative fines under GDPR levied on the third-party: in the worst case, compensation claims may amount to multiples of the GDPR penalties.

Finally, data breaches may also trigger regulatory penalties under the other new European regulations—ePR, PSD2 and AMLD4/5—and may attract separate fines under those in addition to the GDPR penalties. There is no potential for a fine under one set of regulations to be used to offset those under the others.

[3]See Methodology Appendix
[5]Assumes GDPR fines at 2% of the median Tier 2 bank global revenues
[4]Assumes GDPR fines of 2% of the median Tier 1 bank global revenues
[6]Assumes average €5 million fine given small size of Tier 3 banks

Breach Management: Best and Worst Case

Best practice breach management is divided into three phases—pre-breach, active breach and post breach. Within each of these phases there is best and worst-case behaviour, with a range of intermediate responses.

Critically, meeting the regulatory minimum response is not necessarily sufficient to avoid significant regulator penalties, compensation claims and reputational damage. Under GDPR the ramifications of a breach will be dependent on the quality of the response, as well as the initial breach. A poorly managed pubilc response to a breach makes an organisation an easy target for regulators.

Any organisation, no matter how well managed, may suffer a breach. In a world in which organisational perimeters are porous with data flowing through them it is inevitable that data breaches will occur. Indeed, another organisation's data breach may create exposure—for instance, where employees, suppliers and customers reuse email/password combinations.

The challenge is to manage these data breaches at speed and with high quality, to minimise the penalties and liabilities under the regulations and to ensure that reputational damage and senior executive liability is limited. However, such management implies significant levels of preparation in advance of the breach occurring.

The following table outlines best and worst case data breach management scenarios.

Under GDPR the ramifications of a breach will be dependent on the quality of the response, as well as the initial breach.

	Worst Case	Best Case
Pre-Breach Preparation	• Personal data is kept in an unsecured fashion without appropriate access control or logging (GDPR Article 1(f)) • Staff are not briefed, trained or drilled on the requirements for data breach management • There are no communication plans in place for dealing with customers and media • There are no communication plans in place for communicating with regulators • There is no customer customer notification plan, no demand forecast, no address file prepared or identity protections available • Customer-facing staff are not trained and / or third-party resources are not engaged to manage customer communication and harm • There are no breach management terms in third-party contracts (GDPR Article 28) • Impacts on partner organisations and supply chain data distribution are not understood	• Personal data is stored in pseudony-mous, encrypted form, access to this data requires use of access control software, all access is logged • There is a response plan ready including: – Analysis of the critical data – Communication plans for notifying regulators within 72 hours (GDPR Article 33) – Communication plans for notifying customers without undue delay if applicable (GDPR Article 34) – Public relations plan for responding to media inquiries and providing updates to the public – Forecast the potential volume of customer calls, emails & social media posts and identify the resources required to meet the demand – Appropriate identity protections for different types of breaches – Third-parties are properly contracted for data breach responsibilities

continued

	Worst Case	Best Case
Pre-Breach Preparation continued	• No testing of data breach responsiveness • No secure customer communications channel • Customers use username/password for access to services (may result in a third-party party breach exposing the organisation to GDPR Article 82 compensation claims)	– Resource planning for customer service representatives to deal with high levels of concerned customer communications and repairing harm – Data breach drills are carried out to test the effectiveness of the response plan – Definition of the active breach management and post breach support offer to customers • Secure customer communication channels created to reduce notification costs and blunt phishing scams that prey on affected customers after a breach • Customers use secure two factor authentication to protect their accounts from attackers using stolen passwords
Active Breach Management	• Regulators are not notified in the 72-hour window from when knowledge of the breach is obtained (GDPR Article 33) • Information about the breach leaks into the public domain without a mitigation plan • Customer services unable to handle volume of calls or deal with the detailed levels of queries • Lack of secure communication channels slows the response, leaves customers exposed to email and text phishing attacks and dramatically increases postal costs	• Regulators are immediately informed and discussions are undertaken to agree the customer response plan • Data breach response plan is initiated, all staff and third-parties are aware of their responsibilities • Customer communication plan is invoked, subject to agreement with the regulators • Media communication plan is invoked, ensuring senior executives are prepared for action • Customer communication uses secure communication channels to ensure customer details are protected from second wave phishing attacks • Inbound communication channels launched and staffed to meet the demand forecast
Post Breach Support	• No post breach support for customers who experience identity theft (potential compensation claims under GDPR Article 82) • Second wave attack causing further breaches which are liable to attract further penalties under GDPR—often occurring twelve to eighteen months after the initial data loss • Third-parties claim fraud damages due to compromised usernames and paswords (Article 82)	• Customer communications handled quickly and effectively with escalations managed and reviewed hourly • Account recovery allows customers to use services securely • Identity theft victims assigned investigators to repair the harm across all relevant service providers • Additional identity protections including third party service monitoring for further instances of identity theft • All customer activity is tracked and reported • Post event review to identify gaps and improvements for future responses

Unplanned responses under GDPR may well lead to further breaches. Criminals will target customers with email and text based phishing attacks—so communicating using these channels is another source of exposure. Postal communications is more secure, but is slow and expensive.

Surprisingly, communication by post is one of the biggest costs associated with a breach response. According to a Ponemon Institute study, it would cost €2.2m to notify 10m affected customers.

The proper management of a data breach, especially the use of two-factor authentication and secure communication channels, will degrade the value of the stolen data to attackers. This reduces the probability of customers suffering further consequential losses and thereby lowers the likelihood of subsequent claims for compensation.

Communication by post is one of the biggest costs associated with a breach response. According to a Ponemon Institute study, it would cost €2.2m to notify 10m affected customers.

Best Practice Breach Management

If we examine in more detail the requirements for each phase of breach response management we can outline the best practice approach that minimises both GDPR and reputational impacts.

Phase	Pre-Breach Preparation	Active Breach Management	Post Breach Support
Expertise/ Manpower	Breach Communication Planning Breach Readiness Analysis Breach Readiness Testing	Implement Communication Plan Scale Breach Response Resources Respond to Customers	Monitor for Identity Breaches Support Identity Theft Clean-up
Infrastructure	Establish Secure Communication Channel	Secure Customer Notification	Secure Customer Communication
GDPR	Mitigation in Place	Notification Performed	Further Breach Risk Minimised
Reputational Management	Communication Plan in Place	Informed Executive Commentary	Customer Identity Protected

Pre-Breach Preparation

- **Breach Readiness:** Breach readiness analysis generates an action plan to ensure any breach is dealt with promptly and that resources are available and trained to deal with specialised customer concerns and identity theft
- **Breach Communications:** Breach communications planning will ensure that all parties involved in regulatory and customer notifications and press communications are fully briefed and aware of their responsibilities
- **Breach Plan Testing:** Breach plan testing ensures processes work in reality, and all parties are versed in implementation of the plan
- **Setup Secure Communications:** Establishing a secure communications channel with customers ensures breach notifications from the company are known to be genuine as well as reducing resource costs

Active Breach Management

- **Activate Plan:** Once a breach is detected the company must activate the breach communication plan by ensuring all parties tasked with communicating are engaged:
  - **Notify Regulators:** Regulatory notification via the designated legal team is required within 72-hours, this should include an analysis of the breach impact and a plan for mitigating the losses suffered by customers
  - **Notify Customers:** If customer data is exposed then customer notification must be performed without undue delay, coordinated with the regulators.This should include an objective for how quickly the company needs to communicate with customers combined with the recognition that the public may be notified at any time by the news media
- **Engage Expertise:** The appropriate specialist, trained resources with expertise in identity theft issues, must be brought on-line rapidly to handle the immediate high volume of specialised customer queries
- **Manage Customer Queries:** The customer response team must handle the high volume of queries and demands in a consistent and managed fashion, noting that attacks are often designed to occur out of hours when customer service centres are at low capacity
- **Recover Accounts:** The customer management processes must ensure that where customers are locked out of their accounts they are able to recover control of them as quickly as possible to minimise the ongoing financial impact on the business

Post breach support is critical and widely undervalued. Post-support breach services help to mitigate regulatory fines under GDPR and minimise the potential for further breaches based on the same data. Properly managed they can also minimise the possibility of ongoing reputational damage and improve customer retention, as well supported customers are unlikely to migrate to other organisations.

Post breach support is critical and widely undervalued.

Post-Breach Support

- **Ongoing Customer Support:** Part of the breach response should include a definition of the post breach support services that customers will be offered. There are a range of options including:
  - **Identity Repair:** If a customer's breached information has been used maliciously support is required to ensure that the customer does not suffer any long term reputational or financial impact
  - **Identity Protection:** Additional identity protections as appropriate based on the risk presented by the compromised data.
  - **Secure Communications:** A secure communications channel throughout the post-breach support phase ensures that attackers attempting to use the knowledge of the original breach to target vulnerable customers cannot expose the company to further GDPR issues.

Best practice breach management minimises the regulatory and reputational risk and reduces the overall cost impact on the business. This is only possible with effective planning to ensure that the right expertise is available, trained manpower is ready to cope with the volume of queries, and secure infrastructure has been deployed to keep notification costs under control and reduce the risk of further breaches.

Mitigating GDPR Impact: Expertise, Manpower & Infrastructure

Successful breach management requires financial institutions to have access to the right expertise, sufficient trained manpower and the appropriate infrastructure to support the communications process. Anything else exposes the institution to the risk of customer and executive loss and potentially the severest GDPR penalties.

We believe requirements can be grouped into three categories:

Expertise
is needed to deal with breach specific issues:

- Supports response planning
- Informs regulator interactions
- Informs customer support
- Advice on identity management

Manpower
to handle the volume of queries generated:

- Resource to cover the rapid build-up in volume of customer queries following the public notification
- Resource to cover the post-breach management issues

Infrastructure
to provide secure communication channels:

- Insecure credentials are not stored and cannot be breached
- Sufficient outbound and inbound communications capacity to absorb the spike in breach volume on top of normal operating volumes
- Breach communications are secure, inexpensive and do not lead to secondary breaches
- Ongoing secure channel for customers to interact with identity management services

How To Mitigate Each GDPR Requirement?

Taken together the right expertise, planned manpower and secure infrastructure forms a significant set of mitigations to the worst impacts of data breaches and regulatory penalties under GDPR.

Phase	GDPR Requirement	Non-compliance Penalty	Mitigating Service
Pre-breach	Failure to plan for a breach, lacking plan or notification strategy (Article 5, 32,33)	€10 million or 2% of global annual revenues	Response Planning, including active stress testing of response (Expertise)
Pre-breach	Lack of a secure communication channel leads to 3rd-party data breaches (Article 82)	Dependent on damage to third-party, but may include liability for third-parties GDPR fines	Implement secure communications channels with 2-factor authentication (Infrastructure)

Breach response	Must inform regulators within 72-hours of discovering the breach, preferably with mitigation plan in place (Article 33)	€10 million or 2% of global annual revenues	Have response plan including regulatory notification process in place (Expertise)
Breach response	Must inform customers of breach as soon as possible (Article 34)	€10 million or 2% of global annual revenues	Have response plan including customer notification process and trained manpower in place, have secure communication channels in place (Expertise, Manpower)
Breach response	Failure to comply with a supervisory authority order under Article 58 (Article 83)	€20 million or 4% of global annual revenues	For example, where the processor is ordered to inform customers of a data breach and fail to do so—requires a communication plan and secure communication channels in place (Expertise, Manpower, Infrastructure)
Breach response / Post-breach	Compensation for impacted persons (Article 82)	Dependent on the damage inflicted on the individual(s)	Need to provide expert advice to affected customers to ensure they minimise their exposure, provide follow up support to minimise impact of subsequent identity theft (Expertise, Manpower)
Post-breach	Mitigation (Article 83)	€10 million or 2% of global annual revenues	The level of fine levied can be mitigated by the measures offered to mitigate the damage suffered by customers. Proper post breach management services form a key part of this. (Expertise, Manpower)

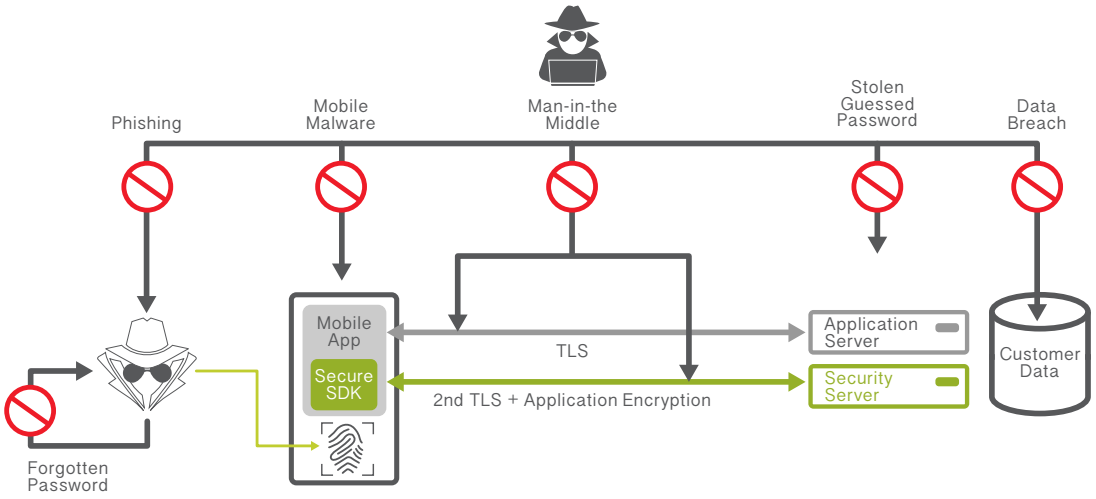
GDPR clearly drives the requirement for the response, but a prompt, clear and well managed process will also reduce the business impact and reputational damage suffered.

Why Secure Communication Channels Are Invaluable

A secure communication channel, underpinned by two-factor authentication, dramatically improves the customer notification and wider process. It makes the process more secure, less expensive and unlikely to lead to a subsequent breach or claims from third-parties for consequential breaches.

The primary benefits of such a channel are:

- **Secure customer notification:** A secure communication channel means that any notification of a data breach can be carried out securely and electronically. This blunts the effectiveness of malicious phishing notifications by conditioning customers to expect communication through the secure channel
- **Cost effective:** Secure communication channels are inexpensive to use, once in place. The alternative is to use postal mail, which is expensive and slow
- **Avoid "contagion" effect:** Eliminate exposure to other people's breaches by reducing reliance on passwords that customers reuse at other organisations. Stop the "contagion" effect of data breaches at those firms, and in turn, help limit the potential for 3rd party damage claims allowed under GDPR
- **Defence against man-in-the-middle attacks:** Using two-factor authentication means that it is harder to gain access to customer data via phishing or man-in-the-middle attacks. This reduces the possibility of any breach occurring in the first place



European financial institutions are already mandated to use strong two factor authentication for access to payment accounts under PSD2. Given this requirement serious consideration should be given to extending this to all customer communication channels.

Conclusion

European financial institutions have largely been addressing the impact of GDPR by focusing on prevention, but have paid less attention to the penalties for failing to deal properly with a data breach when one occurs. The highest risk item in the GDPR is the 72-hour breach notification requirement, and banks are not mitigating this.

The virtually simultaneous introduction of GDPR and the other new EU regulations on the payments industry—PSD2, ePR and AMLD4/5—compounds the challenge. They expand the definition of personal data, increasing the amount of data that has to be stored, mandating new third-party interfaces to allow data to be accessed, and significantly raising the penalties for the data being breached.

GDPR requires regulators to consider a whole range of factors if a breach occurs; they must be notified within 72-hours and customer notification must be prompt, backed up by a robust plan and offer ongoing support to the impacted consumers who are now empowered to sue the organization responsible for a breach.

Our analysis has revealed that European financial institutions are facing approx. €4.6 billion in fines over three years if they don't take proactive steps to mitigate these factors.

GDPR also allows customers and third-party organisations who suffer damage because of a breach to sue for compensation. Where a breach is not contained properly the levels of compensation could easily outstrip the regulatory fines.

Critical to this containment is the pre-breach introduction of secure communication channels with effective two factor authentication. Done properly this degrades the value of customer data to an attacker, removes the possibility of fraudsters targeting affected customers with phishing attacks, and significantly reduces the possibility of breached data being used to access other companies' systems.

We have shown that best practice breach management, with the right infrastructure, expertise and manpower, can significantly reduce the level of regulatory fines.

Institutions that rely on their own general purpose in-house customer services teams are likely to find them overwhelmed by the volume and nature of the customer calls—leading to loss of customers, bad media coverage and ultimately the loss of senior executives.

It is critical that financial institutions do not solely rely on preventative measures to manage their GDPR requirements. A home owner may make every attempt to fireproof their house, but would be foolish to assume that means they do not need home insurance. Similarly, executives need to ensure the proper contingency plans are in place to handle a breach when it occurs, even if they believe that the chances of this are remote.

Proper breach planning will reduce the level of regulatory fines, minimise the possibility of significant compensation claims, help retain customers and maintain profitability and reduce the chances of reputational damage and executive loss.

It is inevitable that some financial institutions will find themselves facing a data breach in the coming years, but the consequences are not inevitable as long as the issues are recognised and the proper steps taken to prepare.

Failing to plan for a breach is planning to fail when it happens.

Appendix: Methodology

We have benefitted from a wide range of high quality sources in the course of our research. In the field of data breach reporting we have drawn on the annual Verizon Data Breach Investigations Report[7], Symantec Internet Security Threat Report[8], IBM and Ponemon Institute Cost of Data Breach Study[9] and Gemalto Breach Level Index[10]. With additional specific research, this has enabled us to develop a rounded picture of data breaches taking place globally and their potential implications.

We then looked more closely at the European banking market, in order to understand the significance of global threats for banks in Europe. Given that the available breach statistics are mostly global, with an acknowledged leaning towards the US[11] in some cases, it was necessary to estimate the relative size of the European banking market. An initial calculation suggests that around 6,000[12] of the 25,000[13] full licensed banks globally are European. Of the top global 100 banks[14] by assets, 32 are based in the EU. On this basis, we have taken a conservative estimate of the EU representing 25% of the global banking market.

It is also instructive to compare the EU and US markets. In terms of GDP, population, penetration rates they are broadly comparable (with the US if anything slightly lower than the EU in some aspects). However, one aspect which is strikingly different is that data breach reporting is currently mandatory in all but a handful of states[15] in the US. It is reasonable to expect that the global statistics, with a substantial US element, may provide an indication of the levels of data breach reporting to be expected once mandatory notification is introduced across Europe under the GDPR.

On the understanding that past performance is never a firm indicator of future behaviour, especially in such an uncertain field as information security, we have endeavoured to provide some conservative estimates of the likelihood of breaches within the market and potential fines these might attract. For our purposes, any EU banks in the global top 100[16] are treated as tier 1. Tier 2 is based on Eurozone banks which are of sufficient scale (by assets) to be recognised as significant supervised[17] entities by the European Central Bank (excluding any already identified as tier 1). Any other banks are taken to be tier 3. We have therefore selected the top 32 banks as tier 1, with a further 75 banks as tier 2, and around 5,000 banks in tier 3.

In order to calculate the expected fines, we have combined the expected frequency of data breach with the annual revenue of a median bank in each of tiers 1 and 2. We have then applied the appropriate level of fines applicable under GDPR. We have chosen the median to limit distortion from the undue weight a small number of exceptionally large banks might produce when included in a mean average.

In order to calculate the likely breach rate in tier 1 banks, we have checked their individual histories of incidents likely to be subject to GDPR fines over the past decade. Historically this has been equivalent to over 8% per annum (on the basis that over 10 years, the most conservative estimate shows 27 recorded breaches across 32 tier 1 banks). In certain jurisdictions, there are minimal reports of breaches, which would suggest significant under-reporting across the region. However, industry surveys[18] suggest that as many as 71% of organisations have suffered some kind of breach over the past year and reports[19] suggest much higher past[20] and predicted[21] figures than we include here.

Tier 2 banks are considered to have a similar likelihood of breach to tier 1 banks: while they present a smaller target, they also tend to have a smaller security budget. They are still of sufficient scale to present a valuable prize for attackers. Tier 3 banks, however, tend to be

much smaller and represent more opportunistic targets. This is particularly the case in certain parts of Europe, where large numbers of smaller banks tend to be the norm.

Our calculations for the number of breaches in tier 3 banks are based on figures from the Verizon Data Breach Investigations Report[22]. We have taken an average of the financial services related breaches for the past 3 years and divided it by four to approximate the number of breaches in the EU (which has 25% of global banks). From this number we have subtracted the number of predicted tier 1 and tier 2 breaches to provide an estimate of tier 3 breaches. Of the 471 finance breaches reported by Verizon in 2016, 30 involved large institutions. These figures, if extrapolated to the European market, are in line with the number of tier 1 and tier 2 breaches we have conservatively predicted. In addition, the IDTRC[23] data breach report includes 52 significant US financial data breaches in 2016. Taking the institutions concerned as broadly equivalent to EU tier 1 and tier 2 banks, this provides further support for our conservative estimates.

In short, we believe that our estimates represent a conservative view of the likely data breach landscape for European banks, post-GDPR. The estimates assume that tier 1 and tier 2 banks will be subject to fines only at the lower 2% level, that the EU market is broadly comparable in size and character with the US market and that existing levels of breaches will neither significantly increase nor decrease. We do not attempt to take into account the likely levels of current under-reporting in Europe or the additional consequential penalties of customers and affected third parties suing to recover losses. It is worth noting that in some countries, there appears to be minimal reporting at present and contraventions only become apparent when exposed in stricter jurisdictions, as has been seen with the large scale AML[24] fines levied in the US. We do recognise, however, that while breaches will almost certainly continue to occur, that supervisory authorities still have considerable discretion about the level of penalty they choose to levy. These figures, therefore, may be improved if banks take the appropriate actions ahead of time to ensure they have mitigation strategies and plans in place.

---

7 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
8 https://www.symantec.com/security-center/threat-report
9 http://www.ponemon.org/news-2/71
10 http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2016-Breach-Level-Index.aspx
11 https://www.symantec.com/security-center/threat-report
12 http://www.eba.europa.eu/risk-analysis-and-data/credit-institutions-register
13 https://www.linkedin.com/authwall?trk=ripf&trkInfo=AQFHkUThl--wrwAAAVyPZepAgS2Hg1aca69iYke9A7YSZ2Ri-J4Sq2r5Z9K1COZGGVT5FH5xgzQIa-PosF-8FIuQF8-inERWqrHFn7vEEoi6GO_tJft8UNbYwr7inqn55XqxtI14=&originalReferer=&sessionRedirect=https%3A%2F%2Fwww.linkedin.com%2Fpulse%2Fhow-many-banks-globally-david-gyori
14 http://www.relbanks.com/worlds-top-banks/assets
15 http://www.lexology.com/library/detail.
16 http://www.relbanks.com/worlds-top-banks/assets aspx?g=8185429b-c98d-484a-9fce-890606c42804
17 https://www.bankingsupervision.europa.eu/banking/list/who/html/index.en.html
18 https://www.solarwindsmsp.com/about-us/press/press-releases/new-solarwinds-msp-security-survey-highlights-overconfidence-lack
19 https://www.computing.co.uk/ctg/news/2411812/all-of-uk-s-major-banks-and-lenders-have-reported-data-breaches-in-the-last-two-years
20 http://money.cnn.com/2014/11/18/technology/security/congress-bank-hack/index.html
21 https://www.scmagazineuk.com/ftse-100-could-face-billions-in-fines-for-gdpr-non-compliance/article/663588/
22 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
23 http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf
24 http://money.cnn.com/2017/01/31/investing/deutsche-bank-us-fine-russia-money-laundering/

Author and Sponsor

About Consult Hyperion

Consult Hyperion is an independent strategic and technical consultancy based in the UK and US, specialising in secure electronic transactions. We help organisations around the world exploit new technology for secure electronic payments and identity transaction services from mobile payments and “chip and PIN” to contactless ticketing and federated identity. Our aim is to assist customers in reaching their goals in a timely and cost-effective way. We support the deployment of practical solutions using the most appropriate technologies and have globally recognised expertise at every step in the electronic transaction value chain, from authentication, access and networks, to transactional systems and applications.

CONTACT: tim.richards@chyp.com

About AllClear ID

Founded in 2004, AllClear ID is the world leader in Customer Security, providing data breach advisory and response services to businesses that aim to protect their greatest asset: customers. As a trusted partner with more than 10 years of specialized experience in data breach response, AllClear ID has helped thousands of businesses prepare for, respond to, and recover from data breaches, including successfully managing the three largest and most complex breach responses in history. The award-winning AllClear ID team is recognised for its expertise, customer service, and guaranteed deployment of large scale response operations in as little as 72-hours.

AllClear ID has expanded to Europe following its acquisition of Norwegian mobile authentication specialist Encap Security. Their combined expertise helps European businesses comply with the new customer security requirements in GDPR and Payment Services Directive 2.

CONTACT: insights@allclearid.com