SAFEGUARDING CUSTOMER DATA IN THE FINANCIAL SECTOR

1. INTRODUCTION

As the financial services sector becomes increasingly digitized, there is amplified focus on data, both in its strategic value, and in how it is handled and protected. The provision of payments, credit, insurance and investment products are reliant on the storage, processing and transmission of data elements that represent financial assets and liabilities, as well as sensitive information about customers.

While the landscape for data management and usage is rapidly changing, one constant is that banks have always been committed to elevated standards in this area. Having a sound data management framework (of procedures, controls and best practices) has always been considered a cornerstone of banking operations, with particular emphasis on (i) protecting data against losses or security breaches, such as unauthorized access by third parties, and (ii) preventing the internal misuse of data, for instance in ways that might distort market integrity. While this is not to suggest that banks are immune from incidents, they consistently outperform other industries in protecting data. Being held to such high standards forms the basis for customers to trust banks with safeguarding their assets.

In a dynamic environment with new players dealing with financial data, it is critical that all market participants can emulate the sound standards that banks already deliver and reach the high security standards that customers have come to enjoy. This is particularly relevant in the context of current “open banking” initiatives that grant third party payment service providers access to customers’ bank account data, generally through Application Programming Interfaces (APIs), or even in less-safe manner. More new players are also starting to provide other bank-like services, including in investments and the wholesale and corporate banking markets. While initiatives such as the recent implementation of Europe’s General Data Protection Regulation (GDPR) mark significant milestones, the safeguarding of customer data performed by financial institutions goes beyond the mere privacy of the individual and the mere compliance with such standards.

This paper explains the key principles and practices that are the heart of how banks manage and protect customer data. These should be essential prerequisites for any other entity wanting to handle customer data, including as a data recipient in an open banking regime.

2. A KEY PRIORITY FOR BANKS

Banks have multiple strong motivations for safeguarding their customer’s data. These drivers have been well entrenched over many years, and continue to feature prominently in institutional culture. While many are rooted in some form of regulation, banks have built on these rules to design additional safeguards that shape their operations.

---

1 In Europe, the new Payment Services Directive (PSD2) has already introduced mandatory requirements for banks in this regard, and the discussion is now on the agenda in other jurisdictions around the world, which are considering how to approach customer data sharing.
Firstly, regulators have been sensitive to the relevance of financial data being safe. There is a multitude of regulations that have stipulated requirements that help to reinforce a strong emphasis on the criticality of data safety, from different types of authorities. These include:

- Specific banking regulations, such as for banking secrecy, IT security and outsourcing
- Bank capital requirements associated with operational risks, including for monetary losses and reputational risk
- Other financial or corporate legal requirements, such as on market integrity and insider information
- Essential infrastructure requirements for security measures and incident notification
- Personal data protection laws and regulations, which are commonly cross-sectoral
- Industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS), mandated and administered by the major card schemes.

Financial institutions also are highly conscious that their data and records commonly qualify as a source of truth on financial positions and transactions, and take this responsibility seriously.

Secondly, banks are subject to active oversight by supervisors and ombudsman offices. This supervision helps to underpin a risk-conscious culture, the application of risk controls, and change management regimes throughout institutions. This has played a central role in the Three Lines of Defense model of risk management, which has been widely embedded across the industry over the last decade.

Thirdly (but perhaps most importantly), banks recognize that their single greatest asset is the trust they have with their customers. Customers rely on banks to take care of their financial assets and to help them plan and manage their financial lives – and this carries immense value within institutions, central to the customer franchises that firms value and seek to grow as the center of their business strategies. Banks recognize that they cannot afford to lose this trust, and they will therefore prioritize the safeguards necessary to preserve that trust, across all customer segments, irrespective of whether they are subject to personal data protection regulations.

3. PRINCIPLES

Banks have therefore implemented substantial safeguards across their organizations, in part for regulatory compliance, but also as a key element of customer confidence and trust. These are not new developments, but rather have been well embedded within institutions over many years.

Across the banking industry, the established frameworks for data safeguards are generally built around four key principles: security; confidentiality (or banking secrecy); preserving market integrity; and transparency.

3.1 SECURITY

Security has always been the primary concern of any financial operation, and in today’s technological context where all financial information is stored and processed in IT systems, IT security is in the spotlight. IT systems, comprised of infrastructure, platform and applications, underpin all banking processes, from day-to-day operations to the development of new functionalities and services, as well as processes in place to assess and manage risk. Financial institutions expend large amounts of resources in their maintenance and updates to

---


3 For example, financial records held or issued by banks are accepted as evidence in court in many countries, with some jurisdictions such as Canada elevating them above other means of proof and setting high hurdles before they can be considered false (see the Canada Evidence Act of 1985); It is also common practice to require a set amount of bank records (often 6 months) as a means to assess the financial status of a person and the legitimate source of their funds (e.g. in loan or housing applications).
ensure they fulfill the increasing IT needs of digital financial services (omni-channel, 24/7/365, data analytics), while maintaining information confidentiality, availability and integrity. The latter is particularly important given that the financial sector is one of the largest targets of cyber-attacks, which are indeed rising in number, scope, and sophistication.⁴

According to Celent, global IT spending in the banking sector is expected to reach USD 264.1 billion in 2018 and increase by 4.2% annually in the forthcoming years, mostly driven by new investment.⁵ Specific security techniques evolve along with banks’ IT systems – from centralized core banking systems to more decentralized systems and cloud solutions – but maintaining a consistent and sound IT security framework is always a key priority.

Such a framework allows financial institutions to identify and assess cybersecurity risks, develop appropriate protection safeguards, detect the occurrence of cybersecurity events, contain their impact and recover to normal operations. The protection safeguards comprise, among others, access controls to physical and logical assets, including identity management and authentication; cybersecurity awareness and training within the organization; integrity checking mechanisms to verify hardware and software; a baseline configuration of IT systems that incorporates security principles, such as that of least functionality; and protective technologies such as encryption or software firewalls. For the detection of and the response to cyber incidents, the information systems and assets are continuously monitored, event data are collected and assessed, and incidents are reported, analyzed and contained.

### 3.2 CONFIDENTIALITY

At the basis of all banking activity is the so-called “banking secrecy” or banking confidentiality.

Implemented differently in various jurisdictions⁶, this generally ensures that banks not only keep the personal information of their customers private, but other financial data as well. As opposed to most personal privacy rules (such as the GDPR), it applies to all customers, regardless of their nature (individual or legal entity).

External banking secrecy ensures that any information related to the business relationship itself is kept confidential from anyone who does not have a legal obligation or the customer’s consent to access it (and therefore a legitimate reason to do so). This starts with the balance on accounts and the transaction data, but also extends to much more extensive information such as investments made and the content of financial advice a customer receives from his bank. Some jurisdictions even extend this to a prohibition of disclosing that a business relationship exists.

Generally, banks consider any information their customer chooses to share with them (or that they share with their customer) to be highly sensitive and worthy of protection. The trust that customers put into banks to safeguard their wealth should under no circumstances be taken lightly and it is this trust that allows these institutions to build a lasting relationship with their customers. The barriers to be overcome before any such information is disclosed without the customer’s consent are high, and often limited to cases of law enforcement, prevention of financial crime and regulatory oversight.

Additionally, the need-to-know principle (also referred to as internal banking secrecy in some geographies) is paramount to banking operations and an integral part of what customers can expect when trusting a bank with

---


⁶ Examples include: UK: Banker’s Duty of Confidentiality as stipulated by the relevant case law (Tournier v Union Bank of England); Germany: ‘Bankgeheimnis’ as part of a German bank’s implicit duties; Austria: Sec. 38 Austrian Banking Act (Bankwesengesetz); Singapore: Cap 19 of the Singapore Banking Act; US banking regulations explicitly cover this right for consumers according to the FTC’s “Safeguards Rule”, implementing the Gramm-Leach-Bliley Act; The FDIC’s rules for consumer data confidentiality are set out at https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/
their information. Much as customers can rely on their data not being shared outside of the bank, it is equally important that access to the data is limited internally as well.

Simply put, financial institutions ensure that only persons which must have access to data to fulfill their duties are allowed to consult and use it. In many cases, financial institutions are prevented from assuming that the data they have can be distributed freely across their organization for other purposes than serving the customer, except where he has given his explicit consent or they have a legal basis for doing so. Even where binding regulations exist which require to share data across the entities and groups, such as the rules governing the risk oversight functions of holding companies in banking groups, the shared data is strictly limited (e.g. amounts and exposures, but not customer names below certain thresholds).

3.3 MARKET INTEGRITY

Beyond keeping data secure and confidential, managing sensitive data in the interest of the market is a staple of banks’ operations. Financial institutions come into contact with information that is susceptible to severely impact capital markets (insider information), an immediate consequence of their position vis-à-vis customers’ financial situations and the service provided. Any type of activity from financing, advising or even processing payments can generate information and knowledge about a customer’s activities and their plans, with potential impacts on share prices and capital markets.

It is a bank’s responsibility to ensure that markets remain fair by not using this sensitive knowledge to their advantage or the one of their employees or customers. Any other behavior could have disastrous consequences by giving one participant a significant and unfair advantage over others, causing a significant loss of confidence in the market and disruption of the system. Being able to determine and classify how sensitive a piece of information is and how it can be used is therefore crucial.

While regulatory requirements are at the basis of these considerations, financial institutions have developed great sensitivity to these issues in their own interest as well. The measures they take to identify what information needs to be severely protected, to identify who holds it and determine if and how it has been used, rank among the strictest internal rules financial institutions set.

In addition to contributing to upholding trust in the integrity of the financial market, the other dimension is the benefit to the customer. The well-established expertise of banks in this space provides customers with the comfort that their highly sensitive data will not only be kept safe, but also that it will not be used to gain a financial advantage or (even worse) used to their detriment. It is this level of trust that allows a close and meaningful cooperation between customers and their banks in developing their business, furthering investments and contributing to economic growth overall.

This principle extends beyond capital markets to banks’ roles in other markets, such as where banks, their employees or their customers could gain an unfair advantage in other areas such as the real estate market – for example, financing development projects in an urban area can be an indicator for an investment opportunity that is not immediately available to others. To prevent the use (or even perception of use) of this type of information for personal advantage, many banks decide to restrict such information from being used or disclosed unevenly. Many even try to mitigate conflicts of interest by restricting access to such investments to their own employees.

This shows how an overarching principle can become common practice across the industry even if the legal requirement where it takes its origin is much more limited in scope. Without the sensitivity and expertise that financial institutions have in handling this type of knowledge, this would not be possible.
3.4 TRANSPARENCY

As previously explained, safeguarding data is essential to build and maintain customer trust. This requires not only ensuring security, confidentiality and market integrity, but also informing customers in a concise, intelligible and easily accessible way how financial institutions hold and use their data. Transparency is at the foundation of trust in any customer relationship, and handling data is obviously a central element of banks’ customer relationships.

Implementation of the transparency principle, in terms of deepness, frequency and push/pull of the disclosures, varies across jurisdictions, depending on the privacy culture, the customer expectations and the regulatory environment. In general, banks publish data privacy notices and policies that disclose what information they capture, the purpose of data processing and whether data are transferred to third parties within or beyond the institution. In addition, banks offer their customers different ways to ask further information or make specific claims regarding how their data is being processed.

4. PRACTICES

The framework in which financial institutions operate requires them to put these high-level principles into actual, every day practice. In that respect, they are treated in the same way as all requirements institutions need to implement, i.e. by devising policies and procedures binding on the employees, setting fixed processes for day-to-day operations which minimize the risks and regularly audit them to make sure that these are effective and followed correctly.

Indeed, banks operate under a framework of Three Lines of Defense: first, the functions that own and manage risks; second, the functions that are specialized in compliance and risk management; and third, the audit and control functions that provide independent assurance. In addition, sound governance structures across the organization make individual staff members accountable at the different lines of defense, and ensure that the board of directors is appropriately reported, directly or through specific committees, and oversees the overall policies.

In addition, financial institutions are held accountable for these very steps by external supervisors, which leads to a considerable amount of effort in their day-to-day operations being dedicated solely to making sure that data is handled adequately. This is especially critical in terms of businesses such as payments, which are not always subject to the same supervisory oversight.

4.1 POLICIES

One measure banks take is drafting a detailed policy on how data should be managed. It typically sets out in detail what data an institution gathers and how it should be stored, before explaining the circumstances under which it can be processed, based on a clear definition of roles and responsibilities within the workforce. These roles in turn determine if and to what extent data can be accessed. Policies also address the security of systems and facilities, the protection of data at-rest and in-transit, response and recovery plans in case of cyber events and the removal and disposition of data.

Such policies are much more than mere paper to be produced in case of an inspection. In fact, they determine the conduct expected from employees. Should a bank employee be found to misuse data and breach these rules, he/she can face monetary and disciplinary consequences because of acting at the detriment of the customer or of market integrity. Many jurisdictions already require that employees lacking in the compliance

---

Footnote:
7 Employees of banks being held to higher standards than in other industries is true for many jurisdictions. See for example: Canada: stipulated in Federal Court Decision in National Bank of Canada v. Lepire (2004) FC 1555; UK: Senior Managers and Certification Regime (SM&CR), see
and ethics area be penalized through their variable compensation, which can be withheld completely in some cases. Breaches of internal policies can also lead to termination of employment, which also strengthen the incentive for employees to follow the rules on safeguarding of data.

4.2 PROCEDURES
Process design of day-to-day operations is another field where the high-level principles come to life. Existing and new processes are usually reviewed by various independent functions within the institution to make sure that sensitive data is not exposed to a risk of misuse or undue disclosure. This includes any process accompanying the launch of a new product. The proponent of a process will usually go through various rounds of review within the organization before it can be formally implemented. In many cases, this involves a review by the information security, data protection or compliance experts. A setup that does not adequately consider data protection and management would not pass the review stage. While it is acknowledged that the best processes can never fully rule out errors or other form of mistake, the risks are still significantly reduced.

Market integrity as described above is implemented through setting up information barriers (so-called “Chinese Walls”). Financial institutions train their employees to recognize insider information and to classify it as sensitive. Projects that might yield such information are ringfenced from the beginning. It is customary to set up separate working areas for the project teams that are inaccessible to other employees, with physical barriers running across trading floors a common sight. The project teams work on separate networks or drives with restricted access. In many cases, communication by traders and employees is monitored by independent functions to ensure that no insider information is disclosed. The same applies to the deals that those privy to insider information make, extending to their own private investments and those of their relatives.

Where information sharing within the organization is necessary, it is customary in many jurisdictions to record what information any employee has and set up insider lists. These are kept and reviewed by independent functions within the organization, which often also monitor the institutions transactions to ensure that the information is not used.

4.3 INTERNAL CONTROL FUNCTIONS
Standard regulatory frameworks for financial institutions require that they set up independent functions in their organization that periodically review and assess the adequacy of their processes and the effectiveness of their risk mitigating measures. This occurs in varying guises and with different scopes through the compliance and audit functions (2nd and 3rd lines of defense respectively).

As with any risk sensitive issue, these reviews cover data safeguarding measures as well. Their employees will periodically gather information within the organization on how the existing processes are implemented, which means reviewing to what extent these adequately address the risk of losing or misusing data. Where this is not the case, this will be raised within the institution to define a remediation plan. The same applies to the assessment of the effectiveness of the measures through sample testing of various results.

The general control framework would also apply to IT systems. These are tested regularly to ensure that:
- they do not contain design failures that allow the loss of data,
- are implemented in a way that safeguards information adequately,
- they cannot be used to circumvent existing information safeguarding processes.

https://www.fca.org.uk/firms/senior-managers-certification-regime/banking; Australia: Banking Executive Accountability Regime (BEAR), see https://treasury.gov.au/consultation/c2017-222462/; EU: compliance with internal guidelines is becoming an increasing part of qualitative factors to be incorporated in the determination of employee remuneration according to Articles 74 and 75 of Directive 2013/36/EC (CRD) and their respective national implementation in the Member States.
4.4 SUPERVISION AND EXTERNAL RECURSE

At the same time, banks are subject to a comprehensive supervisory regime. As part of their mission to ensure the stability of the financial system, public authorities will oversee the soundness of a bank’s organization. In many jurisdictions, the benchmarks for this determination include the measures taken to protect IT systems and customer financial data, even where these requirements are not part of statutory law. Supervisors will pick up if a financial institution shows deficiencies in these areas and require these issues to be addressed. As recent developments have shown, the severity of the scrutiny by public authorities is set to increase further. Customers and the financial market overall can take comfort in the fact that banks and financial institutions are held to these standards and will be accountable if they are unable to reach this standard.

In addition to the above, customers who still feel that their data is not handled adequately have multiple resources and places they can turn to. The ombudsman system for example ensures that customers can turn to an external adjudicator, which will try to resolve a dispute between the bank and its customer in a setting that is less formal, cheaper and less confrontative than the traditional legal proceedings (which are of course open as well). In any case, the aim is to settle such matters through a channel that customers (especially individuals) might be more inclined to use. That system is open to data management issues as well in many jurisdictions.

4.5 OUTSOURCING / 3RD PARTY MANAGEMENT

The reality of financial services is that institutions often rely on specialized partners to provide some parts of a particular service, for organizational and economic reasons. Outsourcing certain functions to external service providers is therefore common practice, with the required disclosure to the customer.

When financial institutions decide to use the services of a third party, they ensure that this third party has no adverse impact on their safeguarding duties, and that customers’ expectations of their bank are still upheld. Banks conduct a thorough risk assessment and due diligence of their potential partners before engaging in the relationship, because the customer’s information must be as safe with the service provider as if it were kept within the financial institution.

Banks typically reserve the right to conduct audits and review the effectiveness of the measures of the third party partners, and contract agreements generally include also the right of financial supervisors to audit the third-party services. To the extent that such arrangements can be burdensome where more dynamic FinTech start-up enterprises are increasingly involved in the future, some new form of supervisory certification may be appropriate – ultimately, it’s the interests of protecting the customer’s data that must continue to come first.

In addition to being held accountable by supervisors for failures of the third party as if they were the institutions’, banks will never jeopardize their most valuable asset, i.e. the customer data, by entrusting it to an entity that cannot provide the same safeguarding standards. These considerations apply identically to processes that have any relevance to insider information.

Customers and the market can therefore trust their bank that wherever it has chosen to include a third party in its service, it has been adequately vetted and the customer can put the exact same level of trust into this third party as the customer puts in the institution.

5 CONCLUSIONS

Open banking regimes can help facilitate innovation and competition in the financial sector, and promote new data-based solutions that empower customers to better manage their financial lives. While financial institutions welcome this added competition, the interests of the (common) customer and the integrity of the market must be safeguarded above all. Customers must be able to continue trusting that their data is handled soundly by
all players engaged in this field, and market integrity and the reputation and stability of the financial system are not put at risk. Where a customer is willing to share his financial information with a new service provider, this should not be translated as a lowering of expectations for the safety of their data.

The principles and practices of financial institutions go beyond regulatory requirements, also reflecting best practices that the industry has developed and refined over time. Supported by robust supervision, this in turn allows customers to trust that their assets are safe, rightly leaving their choice of provider to performance and economic attractiveness.

It is therefore critical that policy-makers ensure the extension of these principles, such that any firm accessing and dealing with financial data can firstly demonstrate that they actually implement sound governance, policies and procedures, comparable to financial institutions. The regulatory framework on financial data safety has sound rationale. While there may be an element of proportionality to some requirements, the fundamental principles for safeguarding customers' data should nevertheless apply regardless of the size, scope or type of operation.

A loss of trust towards the providers of financial services (incumbents and newcomers alike) will otherwise have disastrous consequences, beyond merely missing the goal of enhanced competition in the financial services market. As past crises have shown, a financial services framework that falls short of addressing these risks will not withstand participants turning away.

For a real open banking ecosystem to emerge where various players compete with innovative offerings for customers, sound and consistent data safeguards are paramount. If incumbents, newcomers and regulators actively and constructively cooperate to ensure customer data safety, this will help grow the open banking ecosystem, create more opportunities and ultimately benefit the customer.
Brad Carr
Senior Director, Digital Finance Regulation and Policy
bcarr@iif.com

Adrien Delle-Case
Policy Advisor
adellecase@iif.com

Pablo Urbiola
Policy Advisor
purbiola@iif.com