pkware.com

Balancing Consumer Privacy Rights with Data Communication Needs

Five Factors to Consider in Commercial Banking

2021

Contents

- Balancing Privacy and Protection across Differing Mandates
- Five Factors to Consider When Protecting Consumer Data across Regulations in Commercial Banking
- Building Multi-Mandate Compliance with PKWARE

The creation and consumption of data are constantly growing. According to Techjury, each individual on the internet created at least 1.7 MB of data *per second* in 2020. The current estimate for how much data is created in a single day weighs in at 1,000 petabytes. Data is everywhere, and the growth trajectory is not set to slow any time soon.

Consumer data is a vital piece of transforming business, from complex issues such as understanding pain points or unmet needs to more general approaches such as personalized advertising. Complexities arise, however, considering that holding data means increased risk of vital data theft. Compliance and regulatory standards such as Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), and Payment Card Industry Data Security Standards (PCI DSS) have long been followed by banks, businesses, and healthcare organizations for security programs. Yet it is only more recently that individuals have become increasingly aware of the amount of data they release to companies, and are now demanding ways to better protect their data and by extension, themselves.

> "Data is everywhere, and the growth trajectory is not set to slow any time soon."

Mandates such as the General Data Protection Regulation (GDPR) in the European Union (EU) and the California Consumer Privacy Act (CCPA) have helped play a part in making individuals more aware of exactly how many places their personally identifiable information (PII) data may be stored and what power they have to control its use. In addition, these mandates are helping consumers—and businesses—understand exactly what PII encompasses.

Surface-level PII includes the more obvious data points one might naturally assume: name, address, phone number, Social Security Number, etc. But PII can be comprised of far deeper information. Quasi-identifiers such as email address, IP address, even credit history can also be considered PII, especially when combined with the more familiar PII data points.

The EU took this into consideration when drafting the Data Protection Directive (DPD) in 1996, defining personal data as any "information relating to an identified or identifiable natural person." This definition functions well to include the obvious identifiers along with comfortably expanding to include any new identifiers created by technology. DPD then laid the foundation for GDPR, which outlines broad data protection for all organizations located in or doing business in the EU.

While the EU's data law runs across all industries, in the US, focus is maintained on specific industries. This more individualized approach certainly helps consider the consumer's experience with their data along with industry knowledge and practices. The downside, however, is fluctuation in defining what is considered personal data and thus the way it needs to be protected. This challenge is most notable for organizations that must adhere to multiple standards based on industry, location, or other factors.

Within the financial services industry, for example, commercial banking often finds itself under the law of multiple overlapping—yet different—privacy mandates that affect how it can store, use, and transmit data. There are 4,978 different commercial banks in the United States, ranging in asset size from $3.4 million to $3.2 trillion USD. The largest banks serve customers in every state, which means that not only do these banks need to adhere to industry mandates, but state-level mandates as well.

Balancing Privacy and Protection across Differing Mandates

Big data is vital to the banking industry, especially when it comes to risk management. Real-time insights gathered from customer data can vastly improve risk management, especially when it comes to:

- Cyber fraud detection and prevention: Feed fraud-detection engines for continuous risk assessment
- Liquidity risk management: Better insights on incoming and outgoing cash flow
- Credit risk management: Improve credit models for both private and corporate customers
- Payment card fraud detection: Analyze transaction patterns to identify fraud

At the same time, holding such vast amounts of big data also presents risk to financial institutions. The banking sector has been historically slower to innovate, and legacy systems cannot always keep up with the growing workload. Using an outdated infrastructure to collect, store, or analyze required data puts the entire system at significant risk.

Anywhere there's data, there's risk, and the bigger the data, the higher the risk. This is supported by the growing number of stringent cybersecurity and data protection mandates for banks and other businesses worldwide that collect and use consumer data.

Because the United States lacks a single, comprehensive federal law to regulate both the collection and use of personal information, the resulting regulations often create overlapping and contradictory protections. Because of this, some US organizations may find themselves at a disadvantage globally as their international counterparts need only adhere to simpler GDPR-like comprehensive approaches. While there could be promise of such a privacy law in the US in the future—the Information Transparency and Personal Data Control Act, or ITPDCA, was proposed in Congress in March 2021—in the meantime, US commercial banks must learn how to balance privacy and protection across the various mandates relevant to the financial industry.

Gramm-Leach-Bliley Act (GLBA)

Also known as the Financial Modernization Act of 1999, GLBA is a federal law that mandates financial institutions detail how customer private information is both shared and protected. Financial institutions are required to communicate to customers how they share sensitive data and inform them how to opt-out of data sharing with third parties, as well as apply specific protections to private data according to the institution's written information security plan. GLBA casts a wide net, including in its mandates any company that is either directly or significantly engaged in financial activities. This clearly involves banks, but also brokerage firms, insurers, and any retailer that issues a credit card or "lay-away" plan.

What It Protects: GLBA covers general PII (name, address, Social Security number, phone number, email address, etc.) along with financial information the mandate considers as nonpublic personal information (NPI): collected information that is not publicly known or available that is connected with providing a financial product or service. GLBA allows financial institutions to share NPI with affiliated companies and service providers, but it must be protected. Regardless of the data sharing guidelines, financial institutions are never allowed to disclose a credit card or account number to another company.

Sarbanes-Oxley (SOX)

In the United States, major internal accounting scandals such as WorldCom, Tyco, and Enron triggered the 2002 enactment of the Sarbanes-Oxley (SOX) Act. SOX implemented strict reforms for all publicly traded companies in the US—as well as wholly-owned subsidiaries and publicly traded foreign companies that do business in the US—designed to improve financial disclosures and prevent accounting fraud. Beyond simply accounting, SOX has an impact on the security of information systems, since the law's covered financial information is processed and stored by IT systems. IT departments are then responsible for creating and maintaining corporate record archives, with special attention to data access and retention.

What It Protects: SOX is not directly related to personal data protection or privacy. However, it is concerned with financial auditing controls, and Section 404 of the act is often the starting point to connecting auditing controls with data protection because it requests that public companies include an assessment of internal controls for reliable financial reporting along with an auditor's attestation with their annual reports. The breadth of protected financial information is wider than just PII. SOX includes the same requirements to restrict access and prevent unauthorized disclosures of financial information.

Payment Card Industry Data Security Standards (PCI DSS)

Since 2006, PCI DSS has been the leading set of security standards for maintaining a secure environment for all companies that accept, process, store, or transmit credit card information. Compliance with PCI DSS involves audits that examine an organization's systems and cardholder data environments to identify vulnerabilities with the overarching goal of preventing data from being compromised. The overall intent is to protect cardholder data and secure modern data technology to protect against ongoing data breaches. Cardholder data is not to be stored unless absolutely necessary; if it must be stored, the data must be rendered unreadable and be protected by layers of security technology that minimized exploitation and risk.

What It Protects: PCI DSS is largely concerned with protecting payment card data. More than just the card number, cardholder data includes every piece of information contained on a customer's payment card, from the primary account number (PAN), cardholder name, expiration date, and card verification value (CVV) number to the information stored on the card's strip or chip for authentication and authorization.

State-Level Data Privacy Laws (CCPA, CDPA, CPA, 23 NYCRR 500)

At their core, state-level privacy laws are all about one thing: understanding the data the company holds. Organizations—from financial institutions to retail—are required to protect the PII they hold on individuals that reside in the specified state, regardless of where the business itself is located. Residents of the states that enforce these mandates have specified rights regarding their data under these laws that the organizations must abide by, such as the right to know what data the organization has on them and why, the right to access their information and either correct inaccuracies or delete specified information. Consumers also have the right under many of these laws to opt out of certain data uses such as targeted advertising and sale of personal information.

What They Protect: Generally, state privacy laws protect PII that identifies, relates to, describes, is reasonably associated with, or could be linked—whether directly or indirectly—to a particular person. This could include: name, alias, address, IP address, email address, account names, Social Security number, driver's license number, license plate number, passport number, and other similar identifiers. Information that is publicly available is generally not included.

Five Factors to Consider When Protecting Consumer Data across Regulations in Commercial Banking

While there are multiple similarities in the data that these various mandates require protecting, there are enough key differences that commercial banking needs to maintain a delicate balance in data protection. Financial institutions have the additional requirements of ensuring data is accurate and can also be corrected on demand by customers. And SOX regulates internal financial data via strict controls on changes to reporting data in order to prevent financial fraud. Thus, the types of data now considered private and secured are expanding. Guidelines are also trending toward granular access rights when it comes to PII data and who can interact with it. IT organizations must review file access rights to assess both PII and quasi-PII that exists in unstructured files to ensure the sensitive data doesn't end up in files, folders, or other domains that have less restrictive authorizations.

With that in mind, commercial banks should consider the following when building protection strategies that comply with multiple mandates and multiple definitions of the data that must be protected for compliance.

What data you collect versus what you need to keep

Avoid additional risk by only collecting or storing necessary information. Banks often use big data to detect fraud, find new customers, offer new products and services to current customers, and learn more about how consumers interact with their services. Data such as name, address, payment card data, or account number may also be collected in recorded customer service calls and converted from audio files to text files. This information is redundant to store on servers, not to mention that leaving the information unprotected in accessible locations adds liability.

Before diving into big data, it's important to have a clearly defined process for collecting and storing data. Having irrelevant data not only takes up valuable storage space on your servers, but also opens you up to additional risk if that data is misused or hacked. If you are directly collecting information from customers, clarify what data you're collecting, how it will be used, and how it will be protected. If you don't need the data, don't ask for it. And if you're no longer using it—for instance, if the individual is no longer your customer or the data is no longer relevant—store it securely for required retention periods, then dispose of it appropriately. This will require establishing data criteria protocols and enrolling the appropriate technological solutions to help enforce them.

Where your data is located

Over the past several years, data has grown exponentially, giving rise to the popularity of cloud data storage, making it easier for larger banks to easily and affordably store vast amounts of growing data, or for smaller banks to store data in a cost-effective way. Outside of cloud, data may also be found in databases, data repositories, data lakes, and even endpoints. It's important to know how data can and should be protected in each location. For example, cloud storage providers assure security once your data is in the cloud, but vulnerabilities exist in the transfer process and must be guarded against. Credit card numbers are not to be stored as is; when they are stored, they must be protected with masking, redaction, or encryption, depending on the audience that must interact with the data.

Data discovery is a vital starting point in cybersecurity. After all, it's impossible to protect what you don't know you have. Employees may save data locally to work on reports and analysis, leaving sensitive information unprotected on their laptop. Data could be stored in multiple locations across the enterprise, making it more difficult to ensure that it is coupled with the correct protection and access rights, or even impossible to confirm that expired data has been completely removed from the organization. Automated data discovery scans can ensure that any time new PII is detected, security teams know where it is and what it is so they can take next steps to protect or delete it.

How you need to interact with the data

The type of protection applied to PII and quasi-PII data may need to be dependent upon who is accessing the information. Production data in core banking systems is typically encrypted. If the data is required for testing, important information such as account number, customer name, and address must be masked. Access to production systems is restricted to ensure that only the applicable teams have access to the necessary data. Yet denying access to entire data sets because they contain—or may contain—sensitive data is counterproductive to an organization's goals. Additional tools are helpful in ensuring the usability of data while maintaining privacy of sensitive information.

Masking data allows the organization to maintain control of its PII while maximizing its most valuable asset: data. A data masking solution will render PII as desensitized or protected, yet leave the data's usability intact. For example, production databases can be copied for non-production use, applying masking that keeps sensitive data protected while still allowing the data to be leveraged for accurate insight and measurement.

> "Masking data allows the organization to maintain control of its PII while maximizing its most valuable asset: data."

Necessary policies to protect data for multiple mandates

Data privacy mandate compliance is generally assessed on an annual basis, but compliance itself must be an ongoing endeavor. Some policies can be determined based on commonalities between mandates—for example, including an "opt out" box on data collection forms to satisfy CCPA and GDPR, and defaulting it to unchecked per GDPR. Additionally vital is ensuring that all privacy policies accurately reflect your institution's privacy practices. Policy alone will not satisfy a compliance auditor.

Here, automated compliance solutions can play a crucial role, providing ongoing discovery, protection, and reporting. Both out of the box policy options and custom setups can accommodate actions to the highest common denominator between mandates, triggering the most secure option when data is found on both endpoints and servers. Protection capabilities such as encryption can qualify who is able to access sensitive information, while masking or redacting sensitive data makes it safe for use in any hands—as well as worthless in the hands of threat actors.

Allowing customers to correct or delete the data you hold on them

While a certain amount of PII is necessary to conduct financial matters, bank customers should not feel coerced into granting continued access to their personal information. Ensure your consumers are aware of and understand the implications of where their data is stored and used within your financial institution. Additionally, you must make it clear that depending on the applicable regulations, customers have the right to revoke your organization's right to access, use, or store their data. A Data Subject Access Request (DSAR) is the most common way a customer will make this request. Ensure that this request form is easy to locate and submit on your institution's website.

Responding to a DSAR can be a time-consuming process without the right tools in place. Simply leveraging a data discovery tool to find what you have on the person making the request is akin to attempting to boil the ocean. Discovery is, in fact, a starting place, but should include other solutions such as indexing that make it easier to call up everything you have stored on an individual, regardless of where it is located. Integrate the right-to-know discovery along with right-to-erasure protection with solutions that can create rules to encrypt, mask, or even delete specified sensitive data when it is located.

Building Multi-Mandate Compliance with PKWARE

PK Protect

Because of the value of PII data stored in consumer banking IT systems, they are a profitable target for cyber criminals. The digitalization of finances has certainly contributed to the wealth of data; subsequently, security incidences that negatively impact the data stored by financial services providers are on the rise globally, giving way to multiple mandates that are similar enough across industries, but with enough minor differences that complying with several at once can prove challenging at best.

PK discovery

For decades, PKWARE has been working with commercial banks and other financial institutions to protect its most valuable non-currency asset: data. Protection starts with location, knowing exactly where all your bank's PII is stored. PK Discovery, a vital application of the PK Protect data protection and security suite, automatically digs deep to find every place that cardholder data is stored. PK Discovery can locate data stored in file systems, databases, cloud repositories, even endpoint devices such as laptops and mobile devices. Once data is located, it must be protected. PK Discovery's findings can automatically trigger action based on established policies for precise data protection.

PK encryption

PK Encryption offers reversible protection via file, email, element-level, format preserving, and transparent data encryption. Information is rendered unreadable to users who do not hold the decryption key—such as threat actors or internal users who are not cleared for that level of data access.

Satisfying audit and compliance requirements also requires data security solutions that work with existing DLP. PK Encryption integrates with DLP for sensitive information discovery and encrypted remediation. It solves problems resulting from uncontrolled encryption, providing the viability organizations require in order to fully address security, audit, and compliance requirements while providing persistent protection for their data wherever it is used, shared, or stored.

PK masking

Some use cases require a mix of statically changing values in databases and files while preserving their business value or masking values for only a specific subset of users. To cover these use cases, organizations can leverage PK Masking's dynamic masking, static masking, and file redaction with more than 50 out-of-the-box templates for masking.

PK privacy Detailed regulations are concerned with unique privacy and operational issues that fundamentally give consumers power of what of their data is collected, stored, and used, as well as the right to request correction or deletion of that data. PKWARE's machine-learning infused PK Privacy software scans all systems and repositories that may contain personal data, then contextualizes the information that is obligated to be protected, indexing identities and the data about those identities.

Vast technological innovations over the past few decades have rapidly increased the capacity of commercial banks and other financial services organizations to capture, store, combine, and analyze customer data from financial situation to preferences, habits, and physical locations. And while these trends can benefit consumers, they expose new risks to banks for fraud and cybercrime if data is not accurately protected or properly used.

About PKWARE

Enterprise Wide Policy Management

PK Protect provides a point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it’s copied or shared outside organizations

Integrated Discovery, Classification and Protection

No other solution has the capability to find, classify and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion.

BOOK A DEMO

PKWARE

PKWARE.com

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204