FINANCIAL SERVICES SECURITY

Financial services security and compliance refers to the responsibility financial service companies have to hold, manage, and protect customers’ money and financial information. It involves adhering to central, state, and local regulations that determine standard levels of security surrounding customer data. Protecting financial customers' assets and information has historically evolved with access.

When assets and information were stored in vaults and transfers were made in physical environments, physical barriers were sufficient. Now that lenders (such as banks and credit unions) and insurance companies provide financial products to customers through financial technology (FinTech), they need to also add security systems that comply with regulations. Governments around the world have different laws, regulations, and technology standards and regulatory changes happen every year to accommodate new threats to the world's financial systems.

Why does security and compliance matter?

Because nothing lives in a silo anymore. Everything is connected digitally. So a threat at one point could impact a handful of other financial service providers. Consider the increase in high-profile financial crimes and data breaches. A breach at 1 financial services business regularly impacts other financial service providers.

Large-scale regulatory requirements, corporate governance, data management strategies, and compliance programs strengthen endpoints (and transfer avenues) of customer data. When all financial service providers meet or exceed regulators' or compliance officers' compliance requirements, there are less entry points for security threats.

Cyber security measures, risk assessments, and continued due diligence protect sensitive information—but no system is foolproof. Continued investments in security technology that keep up with new regulations can keep financial services organizations ahead of security threats.

What are the challenges for financial services?

Convenience and customer expectations

The banking industry has made strides moving from a traditional brick-and-mortar model to align with today's convenience and functional expectations. However, technology and customer sentiment are moving faster than government regulatory oversight of the expanding set of digital features, so banks face a challenge to adapt to customer demand while still adhering to regulations that are slow to change. Additionally, new players in financial services are moving quickly to fill any void, challenging established firms to remain competitive.

Data protection

Data fraud and breaches are always risks when digital information becomes more convenient to access. Data is transmitted over many points before it reaches its final destination—and each point presents a potential security risk. Mobile applications are especially easy targets. The app itself and the server it sits on may have vulnerabilities that can be exploited. User behavior can also contribute to the risk.

Government regulations, such as the General Data Protection Regulation (GDPR) in the European Union (EU) attempt to address many of these points of vulnerability, even as data is transmitted across international borders.

Institutional mindset

Changing the mindset of the financial services industry presents additional challenges. The financial sector is cautious about changing from a business model that works reliably to one that, in its point of view, poses risks. The rush to offer consumers more convenience without addressing security risks can have disastrous consequences, but if security processes make the user experience more difficult, customers will look for easier ways to accomplish their tasks. Maintaining this delicate balance is a daunting challenge for even the most innovative and forward-thinking companies.

Public trust

Addressing consumer perception is just as important as the adoption of technology. High-profile data breaches over the years have cultivated an atmosphere of public mistrust toward any company that handles personal data. Trust is easy to lose, and difficult to repair. Customers want assurance that their information is in safe hands. Financial services firms should be as transparent as possible on how they're keeping information safe from cybercrime and data breaches to cultivate trust.

Consumer awareness and education

Educating customers on how to protect themselves is probably the most important element in a productive and safe banking experience. Keeping consumers updated on what to look for to protect their information, and what to do in case of a breach can improve the relationship between bank and customer. This information changes as new technologies and threats are introduced, and keeping consumers informed will go a long way toward attracting and retaining customers.

How should financial services secure data and maintain compliance?

How the financial services industry addresses risk and maintain compliance. Government institutions, companies, and organizations worldwide invest heavily in anti- money laundering, risk management, and compliance processes.

Here are some security options used to meet financial services compliance requirements.

Encryption

Sensitive data goes through an encryption process—converting it into code that can only be deciphered by using the correct decryption key. However, encrypting, verifying, and decrypting data takes extra time and processing power. To speed up ever-increasing amounts of data processing, banks are upgrading and expanding their existing IT infrastructures or implementing new systems that are more flexible and robust to accommodate faster data encryption that easily scales.

Multi-factor authentication

Logging in using multiple forms of authentication is becoming a popular option for more than just financial services websites. The user enters a password or PIN, triggering a request to send a code via text message to a previously registered device. The code contains a set of randomly-generated characters that the user enters to complete the log-in process.

Data storage and distribution

Storing data in one place is no longer a safe option for businesses, even those that rely on cloud services to store digital information. Reliance on a single provider creates a concentration risk—making the data vulnerable to breaches. Distributing storage and functions in separate pieces over several providers dilutes the risk, making it more difficult for criminals to access.