



2017 COMPLIANCE UPDATE

Preparing for the Year Ahead

November 2017



About the Presenters



Today's Co-Presenter:

Melody Joy Hart, CPA, CTP, FP&A
Senior Consultant
Strategic Treasurer

Practice Areas

- Treasury Technology
- Treasury Security Assessments
- Security Training
- Corporate Compliance
- Financial Risk Management
- Bank Connectivity & Onboarding
- Bank Fee Management



Strategic Treasurer was founded in 2004 by Craig Jeffery, a financial expert and trusted advisor to executive treasury teams since the early 1980's. Partners and associates of Strategic Treasurer span the US, the UK, and continental Europe.

This team of experienced treasury specialists are widely recognized and respected leaders in treasury and risk management technology consulting. Known for their expertise in treasury technology, risk management, and working capital as well as other cash management and banking issues, they efficiently identify issues, creatively explore ideas and options, and provide effective solutions and implementations for their valued clients.



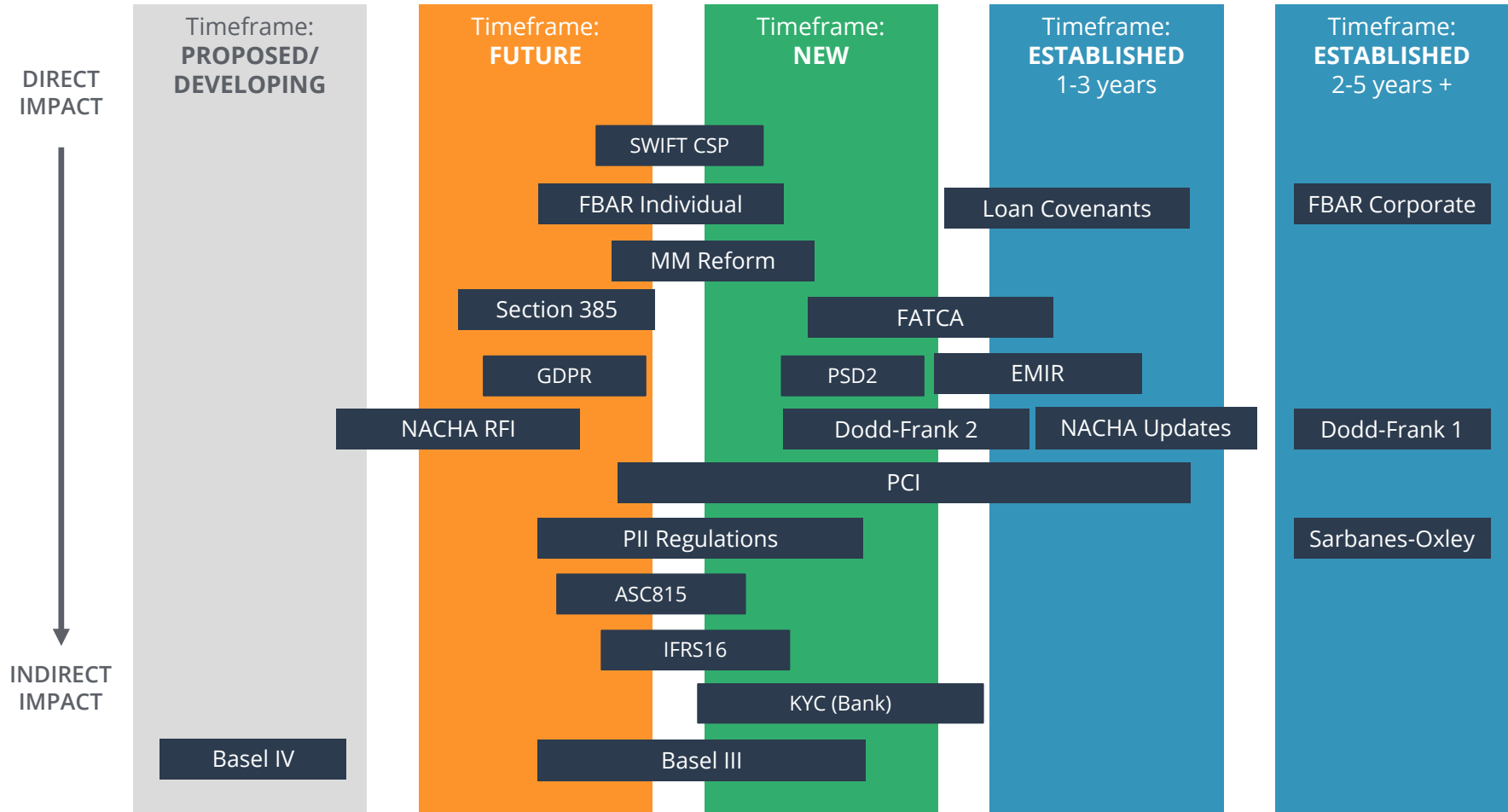


Topics of Discussion

- **Regulatory Landscape Overview**
- **GDPR**
 - What is it?
 - Key Principles
 - Implications for Treasury
- **SWIFT CSP**
 - Overview & Key Points
 - Implications for Treasury
- **KYC Impact on Corporates**
 - What is it?
 - A bank's problem, a corporate's headache
 - A look forward
- **Section 385**
 - Overview & Key Points
 - Implications for Treasury
- **FBAR**
 - Overview & Key Points
 - Implications for Treasury
- **Final Thoughts, Q&A**



Regulations Landscape: Where We Stand





General Data Protection Regulation (GDPR): What is it?

Data Protection Directive



22 Years Old – adopted in 1995. Originally introduced in order to regulate the processing of personal data within the EU.



This directive was outdated and in need of an upgrade to address changes in technology/information processing that have occurred.



May 25, 2018 – GDPR released with the intent to strengthen and unify data protection for all individuals within the European Union (EU).

General Data Protection Regulation (GDPR)

- ➔ Controls personal data of EU residents
- ➔ Regulates how data is handled
- ➔ Affects any organization that does business in or with EU regardless of where the organization is located

General Data Protection Regulation (GDPR): Key Terms



Data subject: An individual who can be reasonably identified, directly or indirectly, by processing their personal data.



Personal Data: Any information relating to an individual that can identify that person directly or indirectly by use of personal data that could also be combined with other data that would make the individual reasonably identifiable. (i.e. Name, address, phone, email address, photo, bank details, IP addresses, device ID's, etc.)



Controller: A person, public authority, or entity that either alone or jointly determines the purpose of the data collection and the means of processing it.



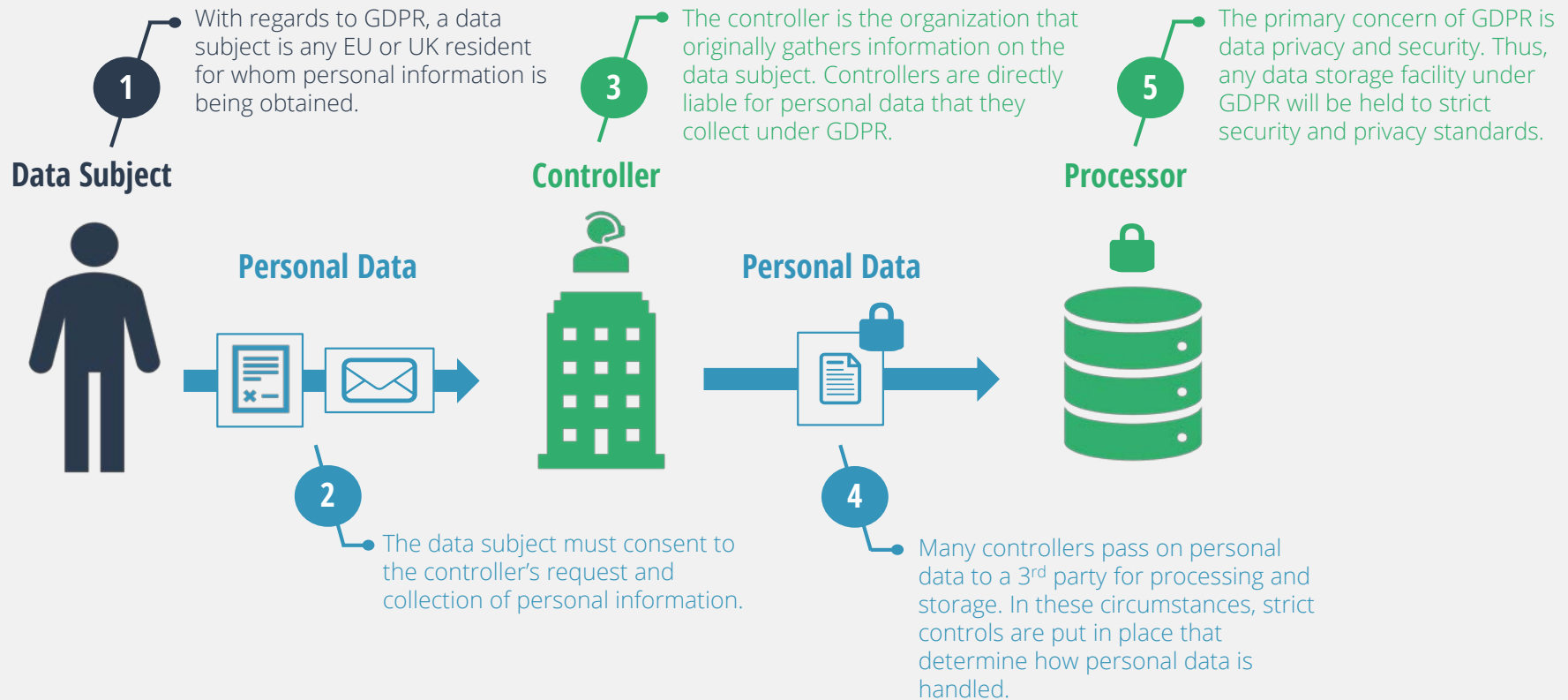
Processor: A person, public authority, or entity which processes the personal data on behalf of the controller.



Data Breach: A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.



General Data Protection Regulation (GDPR): Process Workflow





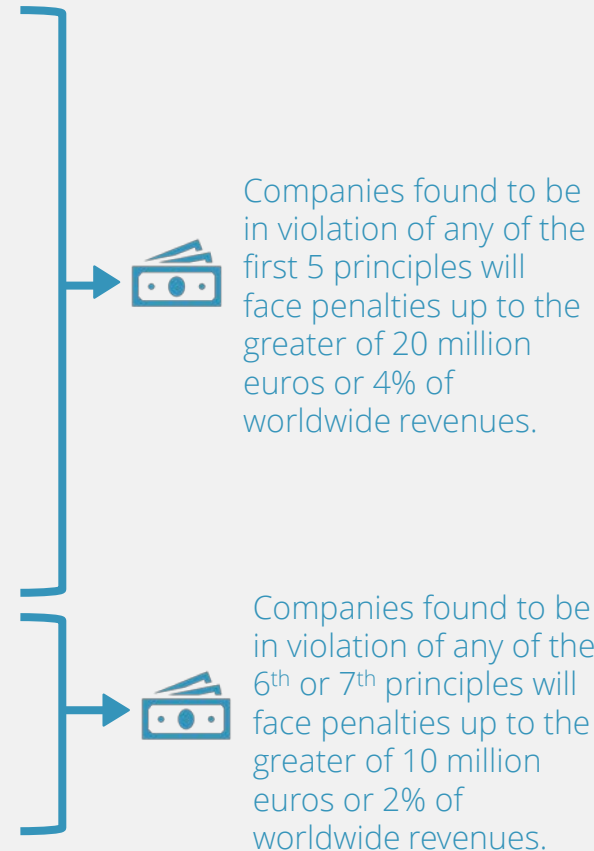
General Data Protection Regulation (GDPR): Principles & Penalties



GDPR Principles

- 1. Lawfulness, Fairness, & Transparency:**
 - Organizations cannot collect personal data without specific consent from individual.
- 2. Accuracy:**
 - Organizations must ensure the information they maintain is accurate and up-to-date.
- 3. Purpose Limitation:**
 - Data obtained from individuals can only be used for its original intended purpose.
- 4. Data Minimization:**
 - Organizations can only collect data that is absolutely necessary for them to acquire.
- 5. Storage Limitation:**
 - Data must be stored no longer than is absolutely required.
- 6. Integrity & Confidentiality:**
 - Personal data must be rendered anonymous or encrypted.
- 7. Accountability:**
 - Companies must give evidence to demonstrate their compliance with each principal.

GDPR Penalties & Fines





General Data Protection Regulation (GDPR): Who is Affected?



While GDPR is aimed at protecting the personal data of European individuals, the regulation has implications for organizations globally.

Firms Located in Europe

Companies headquartered or with locations in Europe.



HR, Payroll, Benefits

Companies with employees of European citizenship.



Firms Conducting Business in Europe



Companies physically located outside of Europe but that conduct business in Europe.


Treasury Operations Involving European Individuals





Treasury-authorities over banking services for individuals located in Europe.

- Signers on Accounts
- Wire Authority
- Access to Lockbox
- Reporting


General Data Protection Regulation (GDPR): Action Items


 **Meet With Business Partners:** As both you and your partners will be collecting data from one another, it is important to meet with banks/vendors the changes that must be adopted to comply with GDPR moving forward.

 **Conduct a Data Audit:** Identify the scope of data collected and stored by your organization as it related to the U.K. and EU, and map the current data processing workflow.

 **Identify Shortcomings:** Compare your current data processing structure and controls against what is required by GDPR, and identify any areas where updates are necessary.

 **Create Remediation Roadmap:** Develop a roadmap of items that must be updated or rectified in order to comply. This roadmap must not extend beyond May 25, 2018.

 **Implement Controls:** Once shortcomings have been identified and a realistic roadmap has been constructed, begin the process of updating your data processing and storage infrastructure.

 **Monitor & Refine:** As changes are implemented, continually monitor the effectiveness of your procedures in complying with GDPR principles. Regular controls testing and risk assessments are both strongly encouraged.



SWIFT Customer Security Program (CSP): Overview & Key Points



A Constant Threat: Cyber crime is not going anywhere. It is here to stay, and will probably increase in severity moving forward.



Evolving Techniques: Recent fraudulent activity has used users' SWIFT credentials to more expediently transfer money/extract funds.



Endpoints Compromised: While the actual SWIFT network has not been hacked, individual users' accounts and access points (endpoints) have been compromised.



SWIFT's Response: SWIFT CSP makes it harder for criminals to access the SWIFT network through users' systems (endpoints).



User Protection: SWIFT's Customer Security Program (CSP) is designed specifically to support their customers in the fight against cyber attacks.



Action Required: The initiative requires action on part of users to comply with the security controls.



Self-Attestation: The program requires organizations to "self-attest" against SWIFT's mandatory security controls using the KYC registry application. Self-attestation is required for every organization with a live 8-character BIC.



Deadline: Users must self-attest their status by December 2017.



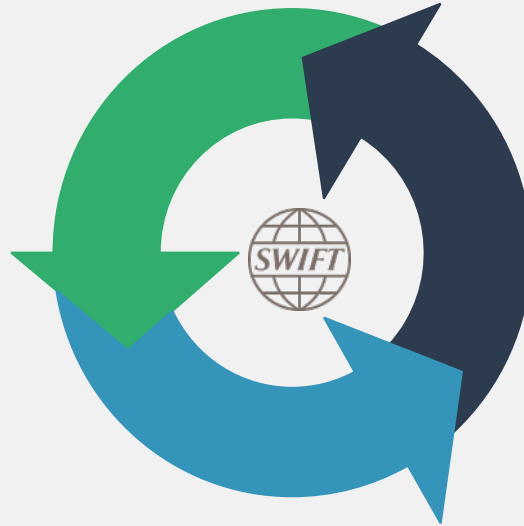
SWIFT Customer Security Program (CSP): Controls Landscape



Your Organization

Secure & Protect

The focus of SWIFT CSP is on securing each “endpoint” to the SWIFT system, which can also be thought of as each individual user. Accordingly, the controls introduced through CSP apply to individual organizations.



Your Community

Share & Prepare

The overall objective of SWIFT CSP is to systematically prevent SWIFT’s network from being used to perpetrate fraud by restricting access to the system and making it harder for criminals to jeopardize user credentials/portals.



Your Counterparts

Prevent & Detect

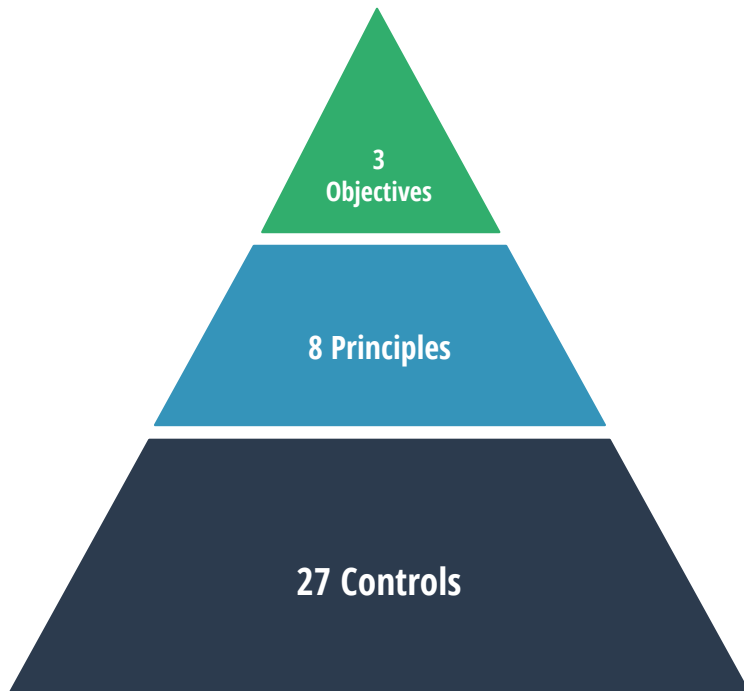
As each organization using SWIFT’s network adopts CSP controls, the result is a lowered risk of fraud across all relationships and a more holistic and robust set of prevention and detection mechanisms.



SWIFT Customer Security Program (CSP): Principles



SWIFT CSP Hierarchy



Controls Framework

- Secure Your Environment
 - 1. Restrict Internet Access
 - 2. Protect critical systems from general IT environment
 - 3. Reduce attack surface and vulnerabilities
 - 4. Physically secure the environment
- Know & Limit Access
 - 5. Prevent compromise of credentials
 - 6. Manage identities and segregate privileges
- Detect & Respond
 - 7. Detect anomalous activity to system or transaction records
 - 8. Plan for incident response and information sharing



SWIFT Customer Security Program (CSP): Key Considerations for Treasury



- **Action Required:** Moving into 2018, any organization using SWIFT should be paying close attention to the following components of CSP.
- **No Fines But...** Organizations that fail to comply with the controls set forth by CSP will not be subjected to fines, but could face other potentially damaging ramifications.



Upcoming Deadline: December 31st, 2017 is the deadline for self-attestation. If you have SWIFT, you should actively be working to ensure your SWIFT controls/processes comply with CSP requirements.



Not a Choice: SWIFT CSP is not a voluntary initiative. It requires mandatory action from all parties to protect themselves from future breaches.



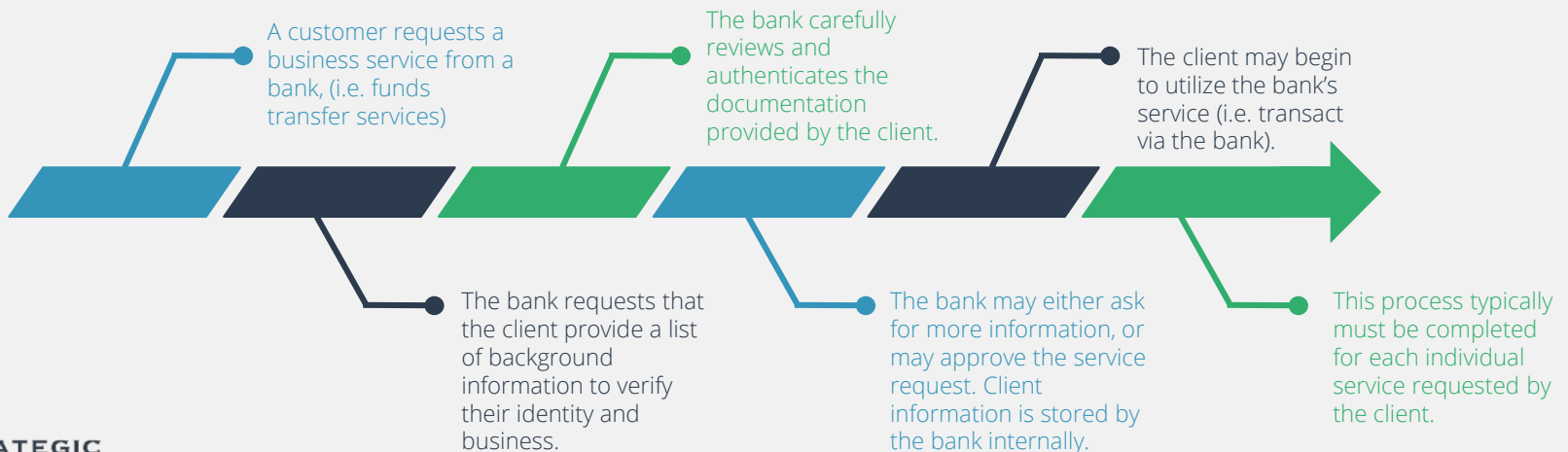
Potential Consequences: Failure to attest may cause other businesses to reduce or block their business with you for security and risk-related reasons.



What to Expect: Organizations on the SWIFT network will have visibility to the attestation and compliance status of other SWIFT users. This means that those users will be able to identify which of their business partners have not met SWIFT CSP security requirements.

Know Your Customer (KYC): What is it? How Does it Work?

- **Overview:** KYC refers to the process of a business or bank investigating and verifying the identities of their clients. KYC requirements were created to ensure that banks and businesses are not transacting or partnering with known criminals or terrorist groups.
- **Introduction:** KYC came about primarily from increased regulation and pressure from OFAC/government agencies to combat terrorism, money laundering, and other criminal activities.
- **Implications:** Result is that banks and businesses must now collect significant information from clients and fulfill tedious documentation requirements before transacting with new or unfamiliar organizations.
- **Current State:** Majority of KYC burden is levied against banks, primarily affects cross-border transactions, particularly in undeveloped or sanctions-stricken areas.



Know Your Customer (KYC): Impact on Banks & Corporates

Banks



Primary Responsibility: Banks shoulder the majority of KYC responsibilities, due to their ultimate authority over the funds transfer process.



Added Steps: This responsibility means that banks must gather more background information and documentation from clients up-front, and often must request information regarding the clients of their clients (KYCC).



Issues Compounded: Added costs for time spent verifying details, delays to business operations, ensuring compliance, etc. is often compounded due to inflexible or legacy technology that cannot handle frequently changing regulatory requirements/updates.



Significant Delays: This drastically increases the cost and the length of time necessary for documentation and due diligence on banking side – it takes ~37 days for retail banks to complete KYC documentation for a corporate client.*

Corporates



Some Responsibility: Corporates and other firms must gather information on vendors, consumers, and other business partners to facilitate bank documentation processes.



TMI: A problem many corporates are experiencing is with regards to KYC is due to their banks asking for too much information or for sensitive information.



Unnecessary Exposures: Banks have routinely asked clients for social security numbers and other highly sensitive/confidential information for purposes of fulfilling KYC documentation. This puts unnecessary exposures and risks onto the corporate as their data is obtained and potentially exposed.



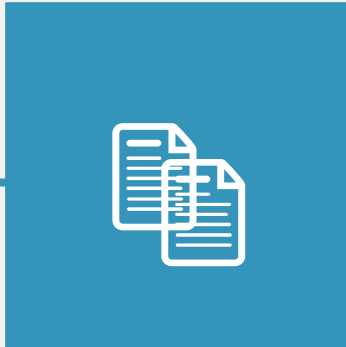
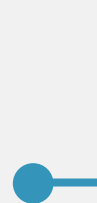
Bank's Burden, Corporate's Headache: As banks gather and store excessive client information, and as the length of time taken for documentation increases, the end result is greater risk for corporates with regards to their data, and delayed services as it takes longer for banks to accept and approve new payment requests, other service requests.

Know Your Customer (KYC): Future Outlook



Increasing KYC Requirements

KYC requirements will not disappear. Continued activity along the criminal and terrorist front, along with increased risk mitigation expectations for banks, will propel KYC forward.



Lack of Automation

Problems faced by both corporates and banks points to a need for streamlined documentation processes.



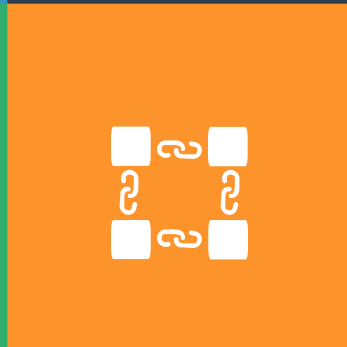
Data Privacy Requirements

GDPR and other data protection requirements may alter how banks can collect KYC data and also what data they are allowed to collect.



Technology Innovations

Moving forward, use of technology such as blockchain may help streamline this process and provide more transparency.





Section 385: Regulatory Overview & Important Developments



Regulatory Background

By way of the 1969 Tax Reform Act, Congress enacted section 385 (Internal Revenue Code) to authorize Treasury to issue regulations to determine whether an instrument should be classified as debt or equity for federal tax purposes.



Policy Shortcomings

Due to limitations of the original section 385 framework, the IRS felt that a loose interpretation of how to classify certain debt and equity-related instruments led to tax evasion.



Recent Activity

Recently, the U.S. government and the IRS have placed debt and equity classifications under increased scrutiny, especially in the context of inversions and other cross-border situations.



April 4th, 2016: Proposed Changes

The United States Treasury and the IRS published proposed regulations under section 385 of the Internal Revenue Code.



October 13th, 2016: Final & Temporary Changes

The Department of the Treasury issued final and temporary regulations for Section 385. Overall, the changes mark some of the most significant changes that the U.S. Treasury has issued in past decades.



2017: Tax Simplification & Deadline Extensions

Activity in 2017 focused mainly on tax simplification initiatives introduced by President Trump's administration, which could impact the finality of 385 legislation. Additionally, a 12-month deadline extension was applied for "documentation regulations."



Section 385: Notable Policy Developments



Proposed Ruling (April 2016)

Bifurcation Rule

IRS has authority during an audit to determine in an instrument that was treated as “full debt” should actually be considered as part debt and part equity.

Documentation Timeline

Originally called for the new changes to be implemented and applicable to all debt issued on or after April 4, 2016.

Cash Pooling & Short-Term Loans

Potential legal implications for cash pooling structures and short-term loans; IRS attempting to crack down on structures that facilitated avoidance of tax protocols or that promoted earning-stripping strategies.



Final Ruling (October 2016)

Ruling Eliminated

The “all-or-nothing” rule remains in effect; the IRS will not be applying partial changes to an organization’s debt and equity classifications at this time.

Documentation Timeline Extended

Changed so that documentation is applicable to new debt issued on or after January 1, 2018 (Now 2019), with a recharacterization effective date of 4/4/2016.

Exemptions & Clarifications

A general exemption for foreign cash pooling arrangements has been enacted that should allow organizations to maintain their pooling structures. Alternative guidelines and exemptions have been provided for domestic pools and short-term loans.



Section 385: Notable Policy Developments



Proposed Ruling (April 2016)

\$50 Million Threshold

Previously, debt below \$50m was excluded from recharacterization, but for amounts over \$50m, the entire sum is included.



Vague Tax “Relevancy” Implications

Original 385 documentation did not provide specification or clarification regarding 385’s application to foreign-issued debt or debt contracts held between foreign organizations.



S-Corporation Status

If debt belonging to an S-corporation were recharacterized into equity, it could jeopardize the firm’s “S-Status” by classifying the debt as a prohibited class of stock.



Final Ruling (October 2016)

Recharacterization Adjustments

The new ruling makes it so that the first \$50m of recharacterized debt is always excluded. Debt will be recharacterized if it is issued to a controlling shareholder.

Foreign Issuer Exception

Final 385 regulations offer exemptions on debt issued by foreign corporations in most circumstances, and instead only apply to debt issued by domestic (U.S.-based) firms.

S-Corporation Exemption

The debt issuances of S Corporations were largely exempt from 385 statutes under the final ruling, thereby eliminating the possibility for jeopardization.



Foreign Bank Account Reporting (FBAR): Key Points



FBAR Regulatory Overview

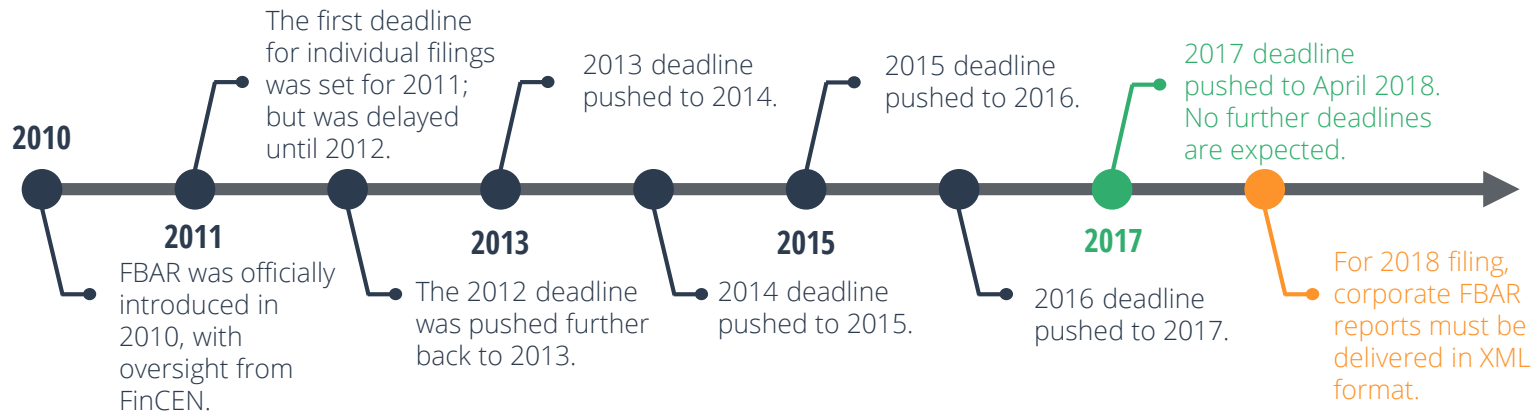
- **Introduction:** FBAR was enacted by the Financial Crimes Enforcement Network (FinCEN), a body of the US Department of the Treasury. The legislation was originally introduced in 2010.
- **Objective:** The primary purpose of FBAR reporting was to target money laundering and tax evasion for U.S. based companies/citizens.
- **Requirements:** FBAR involves 3 types of filing; standard corporate filing, individual filing for no financial interest, individual filing with financial interest.
- **Repetitive Extensions:** The deadline for individual filings for employees with no financial interest has repeatedly been postponed. This extension involves corporate signers that are U.S. citizens and have authority over foreign bank accounts.

FBAR Violations & Penalties

- **Non-Willful Violations:** \$10,000 fine for violations considered non-willful.
- **Willful Violations:** For violations deemed to be willful, the penalty is the greater of either \$100,000 or 50% of the account.
 - For violations are found to have occurred for multiple accounts, each account will be penalized separately.
- **Criminal Violations:** Any criminal Intent associated with the failure to file an FBAR will result in up to \$250,000 in fines, 5 years in prison, or both.



Foreign Bank Account Reporting (FBAR): Key Developments



- **History of Delays:** This extension builds upon a series of deadline extensions that have been occurring for a number of years. (8 prior extensions).
- **Another Extension:** Previous deadline had called for corporate filings for individual signers on foreign accounts to be completed by April 2017.
- **New Deadline:** Deadline has since changed to 4/15/18 for all previously unfiled years (2010-2017).
- **Projections:** Not expected to see any further delays or deadline extensions.
- **Formatting Changes:** Corporate filings must now be completed in the XML format.
- **Action Required:** Organizations should continue collecting FBAR data, plan for the April 2018 deadline, and ensure their reporting processes comply with XML formatting requirements.

2018 Outlook on Compliance

- **Heightened Risks:** Risks faced by organizations, especially along the cyber front, are constantly increasing. Criminal activity and fraud are playing ever-increasing roles in shaping the compliance environment.
- **Stricter Controls:** Regulatory bodies are reacting to these escalating cyber threats by introducing stricter requirements and controls, many of which have significant implications for both banks and corporates.
- **More Regulation:** While there have been initiatives by the Trump administration to reduce regulation, there are already more anticipated regulatory updates and introductions. The current trajectory appears to involve even more regulatory requirements in the future, which will most likely involve fines or penalties for non-compliance.

2018 Action Items

- **Identify Your Exposures:** As the regulatory landscape continues to progress, it is important to obtain a clear picture of which regulations are affecting you or will affect you, and the specific areas in which you are impacted.
- **Act Now:** With large penalties being assessed against firms for non-compliance, it is important to be proactive in establishing the appropriate controls and framework to comply with new regulations, especially if failing to do so could result in a penalty or other risk.
- **Stay Informed:** With regulatory updates being released all the time, it is imperative that you stay abreast of changes as they occur and investigate potential developments to ensure you are not surprised by new legislation.

 Further Knowledge



Take the 2017
Compliance
Survey



COMPLIANCE
Survey

 **STRATEGIC
TREASURER**
Consultants in Treasury

2017 Rapid Research Survey
Less than 5 minutes





Melody Hart, CTP, CPA, FP&A
Senior Consultant
Strategic Treasurer

Email: mhart@strategictreasurer.com
Direct: +1 678.466-2226

EMPLOYEE TRAINING
TREASURY SECURITY
ONLINE VIDEO COURSE

TRAINING · TESTING · DOCUMENTATION
Persistent · Updated · Subscription-Based

SecureTreasury™

IGNORING THE THREAT IS **NOT AN OPTION**

