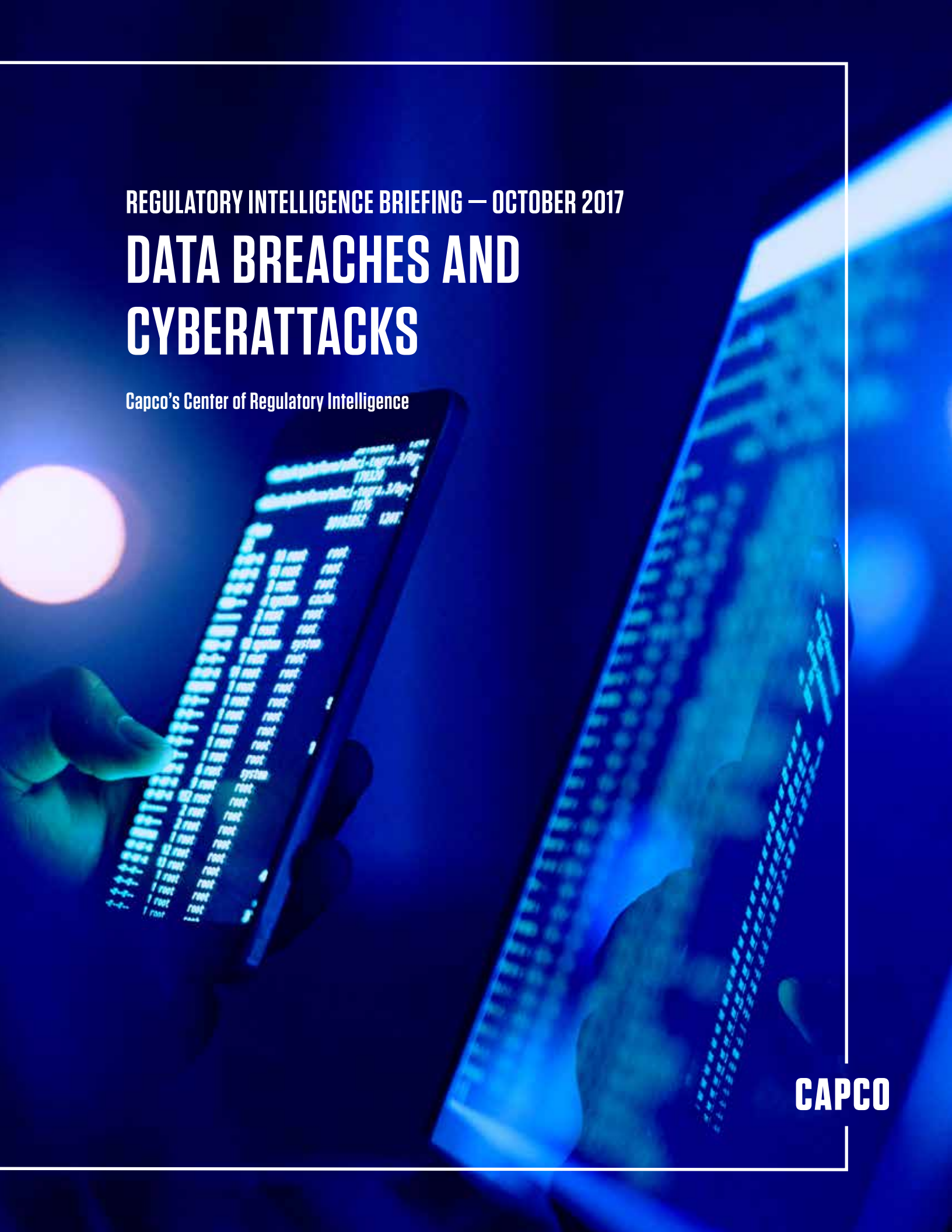
REGULATORY INTELLIGENCE BRIEFING — OCTOBER 2017

DATA BREACHES AND CYBERATTACKS

Capco's Center of Regulatory Intelligence



CAPCO

IN THIS ISSUE

EDITORIAL NOTE FROM THE MANAGING DIRECTOR, CENTER OF REGULATORY INTELLIGENCE 3

REGULATORY ROUNDUP 4

CONGRESSIONAL HEARING SUMMARY: DATA BREACHES 5

FOCUS: DATA BREACHES AND CYBERATTACKS 8

BENEFICIAL OWNERSHIP RULE AND LESSONS LEARNED FROM THE ACAMS CONFERENCE 20

CONTACT US 25

EDITORIAL NOTE FROM THE MANAGING DIRECTOR, CENTER OF REGULATORY INTELLIGENCE

PETER D. DUGAS
MANAGING DIRECTOR, CENTER OF REGULATORY INTELLIGENCE

Peter has more than 16 years of government and consulting experience in advising clients on supervisory matters before the U.S. government and in the implementation of enterprise risk management programs. He is a thought leader in government affairs and regulatory strategies in support of banks and financial institutions compliance with the Dodd-Frank Act and Basel Accords. Prior to joining Capco, he served as a director of government relations at Clark Hill and in senior government positions, including serving as a deputy assistant secretary at the United States Department of the Treasury.

A recent data breach of a major consumer credit reporting agency shocked consumers and institutions worldwide when it became apparent that hackers had accessed personally identifying information of over 145 million people. The highly sensitive data — information that banks, insurance companies and other businesses use to identify consumers — included full names, Social Security Numbers (SSN), birth dates, addresses and, in some cases, driver's license numbers. But this breach is only one of many recent high-impact cyberattacks. And with this increase in cyberthreats, institutions are wondering not only what they can do to protect themselves, but also what a security breach of this kind could mean for their institution as a whole if a hacker makes them a target.

This month's Regulatory Intelligence Briefing (RIB) discusses current trending topics related to data breaches and cyberattacks. First, for our congressional hearing summary, we discuss the recent hearings on this specific breach and provide an overview of some proposed legislation for data protection, consumer notification and cybersecurity supervision, among other trending conversations in Congress.

For our feature article, we begin with an explanation of how these types of breaches occur and the applicable existing rules and regulations with which financial institutions are required to comply. Then, four of Capco's Managing Principals provide their takes on these types of cyberhacks: as the first expert to weigh in, I provide a focus on how lessons learned from recent breaches are affecting legislation in both houses of Congress.

Next, Managing Principal with a focus on Cybersecurity and Resiliency, Scott Ramsey, gives actionable tips for how to ensure system protection, including how to think like a hacker to better understand the threat. Our Managing Principal for Compliance in the Northeast, Marianne Byrne, then explains how to implement and guarantee an effective compliance management system.

Finally, Managing Principal for Consumer Finance and Fair Banking, Robert Cardwell, explains the implications of a breach on Fair Credit Reporting Act requirements. We end with a look at some non-binding guidance that regulatory agencies have published to provide clarity and direction to the entire financial field with regards to cyberthreats.

With the Financial Crimes Enforcement Network's (FinCEN) beneficial ownership rule coming into effect in May, and following the September 2017 Association of Certified Anti-Money Laundering Specialists (ACAMS) conference, our second article focuses on the implementations of FinCEN's rule and the issues surrounding its requirements. One such detail relates to the 25 percent ownership requirement that calls for enhanced due diligence to investigate the natural persons behind legal entities.

The regulations and recommendations regarding these issues continue to transform and develop. Capco's CRI team will keep you updated on all significant changes as they progress.

REGULATORY ROUNDUP

Regulatory and Compliance Alerts

CFPB Finalizes Payday Loan/Debt Trap Rule

On October 5, 2017, the Consumer Financial Protection Bureau (CFPB) finalized a rule on payday, vehicle title and certain other high-cost installment loans. The rule is intended to stop payday debt traps by requiring lenders to determine upfront whether people can afford to repay their loans. The rule also curtails lenders' repeated attempts to debit payments from a borrower's bank account, a practice that racks up fees and can lead to account closure. **The rule is effective 21 months after publication in the Federal Register.**

Treasury Releases Second Report on Core Principles of Financial Regulation

On October 6, 2017, the Department of the Treasury (Treasury) released a report titled *A Financial System That Creates Economic Opportunities — Capital Markets*. The report is the second in a series of reports, in response to Executive Order 13772, covering various segments of the U.S. financial system. This report specifically covers the capital markets sector and recommends several areas for regulatory reform.

OCC Issues Bulletin on Impact of Illegal Practices on CRA Rating

On October 12, 2017, the Office of the Comptroller of the Currency (OCC) issued a bulletin to publicize *Policies and Procedures Manual* (PPM) *5000-43*. The manual sets the OCC's policy and framework for determining the effect of evidence of discriminatory or other illegal credit practices on the Community Reinvestment Act (CRA) rating of a supervised institution.

Agencies Issue List of Key Data Fields for HMDA Supervision

On October 17, 2017, the Federal Reserve Board (FRB) issued a Consumer Affairs Letter to communicate the key Home Mortgage Disclosure Act (HMDA) data fields the agency will use to support the efficient and effective evaluation of a financial institution's compliance with HMDA requirements. The FRB acted in coordination with the Federal Deposit Insurance Corporation (FDIC) and Office of the OCC to designate these key fields.

CFPB Outlines Principles for Consumer-authorized Financial Data Sharing and Aggregation

On October 18, 2017, the CFPB outlined principles for protecting consumers when they authorize third-party companies to access their financial data to provide certain financial products and services. These principles are intended to help foster the development of innovative financial products and services, increase competition in financial markets and empower consumers to take greater control of their financial lives. The principles reiterate the importance of consumer protection to all stakeholders that provide, use or aggregate consumer-authorized financial data.

NCUA Enhances Due Process in Supervisory Review Committee Appeals

On October 19, 2017, the National Credit Union Administration (NCUA) Board announced a final rule to create better due process in appeals of material, examination-related supervisory determinations. **The rule is effective January 1, 2018.**

CONGRESSIONAL HEARING SUMMARY: DATA BREACHES

In early October, Congress held two hearings examining a recent major cybersecurity breach. These hearings took place in the House Financial Services Committee on October 3, 2017, and the Senate Banking, Housing, and Urban Affairs Committee on October 4, 2017. During both hearings, Rick Smith, Adviser to the Interim Chief Executive Officer and Former Chairman and Chief Executive Officer of Equifax, testified.

While much of the hearings focused on the recent breach and how the consumer credit reporting agency handled it, there were many legislative and regulatory themes throughout the dialogue. This article highlights some of these trends and the types of legislation that have been introduced in Congress.

Data Protection

This is not a new discussion topic on the hill. As we have seen this year, through the Executive Order on Cybersecurity and other developments at the state level, legislatures are putting an increased focus on cybersecurity, particularly on data protection. The most recent major breach, and subsequent smaller breaches over the past few weeks, has highlighted that this issue will not be going away. Cybersecurity at financial institutions, and other types of firms, is not just about stopping hackers from stealing money from accounts, but also about protecting the sensitive personally identifiable information to prevent it from falling into the wrong hands.

Since the beginning of October, three bills have been introduced related to data protection:

1. Rep. Debbie Dingell (D-MI) introduced the Data Protection Act of 2017 (H.R. 3904). The bill is simple; it would require the Federal Trade Commission (FTC) to prescribe rules for covered entities to secure sensitive personally identifiable information against a security breach.

2. Rep. Janice Schakowsky (D-IL) introduced, on the same day, the Secure and Protect Americans' Data Act (H.R. 3896), which provides a more robust framework for what security polices, practices and procedures the FTC must promulgate into regulation. The bill also covers how to notify individuals whose personal information is reasonably believed to have been accessed in a security breach.

3. Rep. Warren Davidson (R-OH) introduced the Market Data Protection Act of 2017 (H.R. 3973) in response to a breach of the Securities and Exchange Commission's (SEC) Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database in September. According to a press release on Davidson's website, this bill is more focused than the other two bills, as it specifically amends the Securities Exchange Act to direct the "[SEC], the Financial Industry Regulation Authority (FINRA) and the Thesys Technologies to accelerate its cybersecurity risk Electronic Data Gathering, Analysis, and Retrieval (EDGAR) database in September. According to a press release on Davidson's website, this bill is more focused than the other two bills, as it specifically amends the Securities Exchange Act to direct the "[SEC], the Financial Industry Regulation Authority (FINRA) and the Thesys Technologies to accelerate its cybersecurity risk controls before collecting data in the Consolidated Audit Trail (CAT) to prevent future hacker attacks."

Security Breach Notification Laws

There is no federal standard related to notification of affected consumers after a security breach involving personally identifiable information. However, according to the National Conference of State Legislators, 48 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted legislation requiring notification of individuals when breaches involve personally identifiable information. The states' laws vary as to whether they apply to private or governmental entities; who is required to comply with the laws; definitions related to the laws; and requirements related to notice.

On September 18, Rep. Jim Langevin (D-RI) re-introduced the Personal Data Notification and Protection Act (H.R. 3806) to set a national standard for notification of affected persons following a data breach. The bill would generally apply to business entities "engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period…" Affected consumers must be notified within 30 days, but the FTC can grant extensions in 30-day blocks. Importantly, the bill includes exemptions from notifying individuals related to data breaches, including when information could damage national security.

SSN as the Identify Verification Standard

In closing his testimony, Smith offered two observations, with the second one supporting the "creation of a public-private partnership to begin a dialogue on replacing the Social Security Number (SSN) as the touchstone for identity verification in this country." The major issue is what form of identification could replace the SSN, an identifier that has been around since 1936.

According to the transcript from a cybersecurity summit in October 2017, White House Cybersecurity Coordinator Rob Joyce spoke about the SSN, calling it a "flawed system." In speaking about the recent breaches, Joyce provided the example that no one has changed their SSN following confirmation that they may have had their information breached. Further in the conversation, Joyce announced that government departments and agencies are gathering information surrounding the use of SSNs and "the vulnerabilities in the cyberworld."

Recently, Rep. Patrick McHenry (R-NC) introduced the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2017 (PROTECT Act; H.R. 4028) that aims to establish cybersecurity supervision in the U.S. and provide for examination of large consumer credit reporting agencies. But, the bill also carries provisions to take effect in 2020 that amend the Fair Credit Reporting Act (FCRA) to prohibit reporting agencies from making any consumer report that contains an SSN or using an SSN as a method of consumer identification.

While we are likely far from the demise of the SSN, some alternate identification methods that may be explored in the coming months include blockchain, biometrics and other digital authentication solutions.

CFPB Arbitration Rule

In response to the breach, the consumer credit reporting agency offered a suite of products to help the aggrieved. However, the initial roll-out contained language barring anyone enrolling in the program from participating in a class action suit. The language was later removed, and according to Smith during his testimony, the initial inclusion was a mistake. However, this opened the door for a discussion during the hearings about the Consumer Financial Protection Bureau (CFPB)'s final arbitration rule. In particular, Sen. Chris Van Hollen (D-MD) pushed Smith for his position on the rule, which was facing an early-to-mid November deadline for repeal by the Congressional Review Act, 60 legislative days from the rule's publication on July 19, 2017. On October 24, the Senate passed the joint resolution of disapproval, and at the time of writing, the resolution is awaiting a signature from President Donald Trump.

Corporate Governance

During the hearings, some members of congress inquired about the consumer credit reporting agency's governance structure. During the House hearing, Rep. Carolyn Maloney (D-NY) and Rep. Tom Emmer (R-MN) brought attention to an institution's "global security officer" report to general counsel, who is a direct report to the chief executive officer. To be clear, this is not an area that has a right or wrong answer. All institutions are set up differently, but what these hearings emphasized is how important corporate governance is and how it can play into an institution's perceived culture of compliance.

FOCUS:
DATA BREACHES AND CYBERATTACKS

As outlined in the Congressional Hearing Summary above, the topic of data breaches has been of particular importance lately. In light of recent events, legislators are attempting to quell fears and strengthen security by both creating federal rules for cybersecurity and exploring alternatives to the types of data information systems store. But even with increased government focus on the issue, for many institutions, the prospect and fear of data breaches have become intense and more personal.

Announced in early September, the breach of a large U.S. consumer credit reporting agency is only one of many recent hacks that have led to illegal access to nonpublic information (NPI). In late September, a large consulting firm confirmed it had suffered a cyberattack that allowed hackers access to clients' personal emails. And going beyond financial services institutions, 2017 has seen numerous ransomware attacks and illegal data hacks on organizations from health clinics to governmental agencies.

The Starting Point: How Did This Happen?

While the sheer magnitude of the consumer reporting agency's data breach garnered the country's attention and derision, the institution's story isn't so different from many others. The "flaw" was a vulnerability left unpatched, and series of missteps in oversight.

According to testimony during congressional hearings on the breach in early October, on March 8, 2017, the institution received an automated message from US-CERT regarding versions of software requiring patches for certain vulnerabilities.

The next day, the breached institution disseminated the US-CERT notification internally, requesting that applicable personnel upgrade their software within 48 hours. However, the vulnerable version of the software was not identified or patched in response to the internal notification.

The following week, the institution's information security department also ran scans to identify any systems that were vulnerable to the issue identified by US-CERT. But, the scans did not identify the vulnerability.

Undetected by the agency's security tools and exploiting this unpatched vulnerability, the hackers likely accessed NPI between May 13 and July 30. By the time the agency's security department observed suspicious network traffic, a huge amount of NPI had been accessed with no way of "getting it back."

Gramm-Leach-Bliley Act (GLBA)

Financial institutions are required, under the GLBA, to "insure the security and confidentiality of customer records and information." Under the GLBA, a financial institution is defined more broadly than other federal statutes and encompasses businesses "significantly engaged" in providing financial products or services, regardless of size. One of the major provisions of the GLBA is the "Safeguards Rule" (GLBA § 501(b)), which requires financial institutions to maintain a robust information security program consisting of the following criteria:

- Designate one or more employees to coordinate the information security program.
- Identify and assess the risks to customer information in each area of the company's operation and evaluate the effectiveness of current safeguards for controlling these risks.
- Design and implement information safeguards to control the risks identified through risk assessment and other testing and monitoring activities.
- Select and retain service providers that maintain appropriate safeguards, through service agreements/contracts.
- Evaluate and adjust the information security program based on the results of the testing and monitoring performed.

Financial institutions are also required to follow security guidelines, detailing, among other things: the risk assessment process; requirements when hiring an outside consultant; sufficiency assessments for policies and procedures; security controls' design requirements; development and implementation of a program for responding to unauthorized access to customer information; circumstances for customer notice; training; key controls' testing; responsibilities of the board of directors; and service providers' oversight.

What Happens after a Breach

The GLBA makes it an institution's responsibility to protect NPI, and there are consequences for simply allowing this information to get into the wrong hands. But it can also be troublesome to think what a hacker could do with NPI once it's leaked.

On September 20, 2017, U.S. Securities and Exchange Commission (SEC) Chairman Jay Clayton released a statement on a 2016 data breach of the SEC's EDGAR system, an online platform that collects and processes detailed financial reports that publicly traded companies submit. According to Clayton, "In August 2017, the Commission learned that an incident previously detected in 2016 may have provided the basis for illicit gain through trading. Specifically, a software vulnerability in the test filing component of our EDGAR system, which was patched promptly after discovery, was exploited and resulted in access to nonpublic information." The SEC was aware of the hack and patched the vulnerability quickly, but once the hackers accessed the NPI, there was nothing the SEC could do to stop them from using it however they planned – which, in this case, was for illegal trading.

In the rest of this article, four of Capco's subject matter experts will provide their perspectives on data breaches and the concerns raised within each subject area. First, Managing Principal of the Center of Regulatory Intelligence, Peter D. Dugas, highlights potential regulatory action and the importance of regulatory change management (RCM). Then, Managing Principal focusing on Cybersecurity and Resiliency, Scott Ramsey, explains what effective human-technology alignment looks like and how to "think like a hacker" in order to better protect an institution. Next, Managing Principal for Compliance Risk Management in the Northeast, Marianne Byrne, provides insight into how to protect an institution through an effective compliance management system (CMS). And while the GLBA is on many institutions' radars when discussing data breaches, Managing Principal for Consumer Finance and Fair Banking, Robert Cardwell, reminds furnishers that the Fair Credit Reporting Act (FCRA) requirements should also be a top priority to protect consumers from identity theft.

PETER D. DUGAS

MANAGING PRINCIPAL, CENTER FOR REGULATORY INTELLIGENCE. FOCUS ON REGULATORY INTELLIGENCE AND TECHNOLOGY

"The New York Department of Financial Services reacted quickly to the recent breach, issuing proposed regulation requiring credit rating agencies to register in the state and outlining prohibited practices, among other things. Additionally, Capitol Hill is already starting to line up hearings to examine the issue and members of Congress have wasted no time issuing their own legislation. This issue affects Americans in every district across the U.S., and it will certainly be a target for congressional attention over the coming months. During this time, financial institutions must be sure to look back on regulations surrounding third-party vendor management and data security, make sure the correct controls are in place, and stay abreast of the evolving regulatory landscape."

In the wake of the recent data breach where over 145 million consumer records were exposed to potential fraud or misuse, companies should expect increased scrutiny from Congress and regulators on information security and cybersecurity programs. Boards of directors, executives and senior leadership of companies who have failed to prevent, detect and monitor for cyber-risks and were subject to a successful cyberattack, have been called before Congress to explain their deficiencies. These explanations have included: the extent of knowledge of the incident; steps taken to prevent and respond to the attack; and even justifications of whether employees had requisite knowledge and experience for their positions, in order to support protecting the company and its sensitive information.

While many companies are saying, "I'm glad that's not me," how many institutions are learning from these cyberattacks and analyzing the victimized companies' responses to ensure their own institutions would be better prepared to respond to government, shareholder and customer scrutiny in the face of this type of incident?

Institutions should use these incidents as an opportunity to remind employees of their obligations under existing laws and regulations; ensure employees are trained on information security and applicable consumer laws; and set a tone throughout the institution on the importance of strict adherence to policies and procedures regarding cybersecurity and associated risks.

The lessons learned regard not only adherence to existing expectations, but also monitoring of proposed legislation and potential causational changes to an institution's business practices. It is important that institutions have a built-in process under their RCM program to monitor proposed and new legislation. The RCM program should include a process for appropriate subject matter experts to review legislation and regulation to determine the institution's related obligations and potential impact to business strategy, products, services and operations.

Given the rare bipartisan outrage over the recent data breach, policymakers agree that companies should be proactive and take appropriate steps to protect their customers' sensitive NPI. In the House and Senate, policymakers have proposed legislation to hold companies that collect consumer data accountable when the information they collected is misused or stolen. The bills also give consumers the ability to have more control over the use of their personal information and provide regulators with oversight over the use and collection of information supplied to consumer credit reporting agencies.

Recent Proposed Legislation

In the Senate, Sen. Elizabeth Warren (D-MA) recently introduced S. 1816, the Freedom from Equifax Exploitation Act. The bill proposes to amend the Fair Credit Reporting Act (FCRA) to enhance fraud alert procedures and provide free access to credit freezes.

In the House, Rep. Patrick McHenry (R-NC) has introduced H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology (PROTECT) Act of 2017. The bill is targeted to "large consumer reporting agencies," but would also impact any institution that relies upon these reporting agencies to make credit decisions. The bill proposes to amend the Federal Financial Institutions Examination Council Act to establish cybersecurity supervision and examination of large consumer reporting agencies, and would also establish uniform cybersecurity supervision and examination procedures

While it would be easy to ignore legislation primarily focused on consumer reporting agencies, these types of laws will be important for banks, credit unions and other types of financial institutions that use these agencies' data. It remains in question how a financial institution would potentially respond to security freezes, delays in material evidence for credit determination, or consumer requests or complaints made to the financial institution rather than the reporting agencies. As in the recent data breach, banks and financial institutions must make decisions on how to respond to regulatory and contractual obligations for a third-party relationship.

In addition to the legislation introduced, Congress has recognized the need for clear guidance from regulators and a harmonization of cybersecurity regulations. Republicans and democrats on the House Financial Services Committee sent a letter to federal financial regulators in August stating that "A broad-based, collaborative effort — among your agencies and with the private sector — is needed to identify, defend against, and counter these cyberthreats." The letter requested that regulators not only synchronize their rules and regulations to reduce inefficiencies and improve outcomes, but also to engage with the states when determining the standards and appropriate framework to make the financial system more resilient to cyberattacks.

It is expected that cyber-risks will grow over the coming years, with hostile nation-states becoming more sophisticated and hackers more adept with emerging technology, such as artificial intelligence or machine learning used to accelerate attack patterns and improve success rates. Congress and regulators are challenged with not only gaining an understanding of the new threat environment, but also crafting legislation that protects consumers and the financial system from both existing threats and unknown future threats.

Capco will continue to monitor the shifting environment and Congressional and regulatory actions, and keep financial institutions appraised of the impact to their information security compliance and oversight programs.

SCOTT RAMSEY

MANAGING PRINCIPAL
FOCUS ON CYBERSECURITY AND RESILIENCY

"Why is it that when a data breach occurs, everyone focuses on the failings of technology and patch management? Updates were not current, patches weren't installed, infrastructure is too complex to track. Have we become so complacent that we forget that in Security, U R IT? At the end of the day, it is the carbon-based unit on the keyboard and monitoring the screen that is accountable. How is it that the "bad actors" could "sit" on internal networks for over a month and not be noticed? Who had "eyes" on the networks, or, were the responsible parties just relying on automated reports and alerts being generated by Security, Information and Event Management (SIEM) products? We need to get back to the basics and realize that neither technology nor people are infallible and that both need to work together to protect and secure platforms, networks and data."

There are two common areas in which people rely too heavily on technology when more human management is necessary.

Security Information and Event Management (SIEM) tools: Information technology (IT) infrastructures are becoming larger and more complex. SIEM tools are being implemented to assist in monitoring for anomalous activities, but they are not enough. Human intervention is necessary to determine if a false-positive is truly that or an activity that needs to be investigated.

Intrusion Detection Systems (IDS): These systems are not being "tuned" properly. Changes occur within the IT infrastructure which require re-tuning of devices. Logs and reports need to be reviewed, and institutions cannot just focus on alerts that the tool produces.

Some red flags for insufficient protection might include not having:

- Information security education, training and awareness programs
- A qualified individual serving as the Information Security Officer
- Information security and cybersecurity as standing agenda items at board of directors' meetings

Some operations that may help prevent a data breach include:

- Requiring multiple-level access controls, both logical and physical, to NPI and resources that interact with it
- Properly implementing, monitoring and tuning SIEM tools, by qualified personnel
- Implementing and enforcing service-level agreements (SLAs) with third parties around access to and data management of NPI
- Monitoring and enforcing data management policies and procedures
- Proactively educating, training and raising awareness regarding security

There are ways to better align humans and technology.

Proper Training: Ensure that personnel are appropriately trained on the use of the technologies that they are utilizing and on which they are relying.

Awareness: Make sure that personnel understand and know what the normal operating parameters are for the technologies in place.

Vigilance: Educate personnel on what to look for that is out of the ordinary or abnormal. Don't just rely on what the technology produces.

Enforcement: When personnel does not adhere to a policy or follow a procedure, make sure to enforce the appropriate consequence.

THINK LIKE A HACKER

Recently, large institutions are the targets and small institutions are gateways to the targets. While smaller institutions generally have the same requirements to comply with regulations as the large institutions, smaller institutions often don't have the budget nor available resources to fully meet these requirements. In many cases, this means that smaller institutions do the best they can and hope it is enough. A hacker will always look for the weakest link in a supply chain and the easiest route to their goal. If the hacker can compromise a smaller institution with a spoofed identify and authenticate into the target, the hacker is where they want to be.

Pre-attack, a hacker will perform exhaustive reconnaissance, which is the most important step. Hackers will gather as much information as they can about a target, including crawling the institution's web site and connecting with executives and employees through social media (e.g., LinkedIn, Facebook). Hackers will then construct profiles of executives: interests, job history, travel routines, vacation schedules, etc., often using social media sites. A hacker may apply for a job with the target or with an outside services company (e.g., cleaning office, washing windows); social engineer the institution's personnel; or request a meeting with the Chief Information Security Officer (CISO) to present "consulting services." A key aspect of the pre-attack stage is that the hacker will open an account. Due to regulations requiring that an institution notify clients if there is a data breach, the hacker now has a sense of security before and during the attack. The hacker will then devise the plan for the attack.

During the attack, the hacker will follow the plan they devised, attempting to obtain trophies such as personal or account information. This may include compromising devices on internal networks; constructing backdoors for later access; and planting logic bombs for misdirection of backdoors. The hacker will exit as soon as possible and cover their "tracks."

The next step is to wait. The hacker must see when or if the breach is made public, holding onto data with no activity for several weeks or months. It is important to remember that hackers have no timeframe for the use of data because NPI never loses its value. Complacency is a "friend" of hackers. At an appropriate time, the hacker will execute a plan for data use. Sometimes, the objective is it to sell off the NPI, usually to someone who needs it for immediate illegal monetary gain. Other times, the hacker holds the NPI to use for their own purposes in the future, including years later in some cases.

MARIANNE BYRNE

MANAGING PRINCIPAL
FOCUS ON COMPLIANCE RISK MANAGEMENT IN THE NORTHEAST REGION

"What better time than now to reassess the controls related to your Compliance Management System (CMS)? The historical data breach should have every member of the C-Suite asking tough questions about their CMS. You may ask, what can be done now that the breach has occurred? The first step would be to assess the pressure points of policies, procedures, monitoring, assessments, testing, reporting, board and executive management oversight and training. Then, identify the known controls within the system, locating the gaps and documenting the residual risk, which will enable a better understanding of how your control system withstood the enterprise impact of the breach. If data is found to be unreliable, institutions will be unable to properly assess risk within their CMS."

Large breaches impact all financial institutions.

This includes banks, non-banks, fintech companies, alternative lenders and consumer credit report providers and users (including human resource groups, staffing agencies, rental companies and more). A compliance goal for every institution is to identify gaps in operations, which are best evaluated through assessments of the institution's products, services, third-party affiliates, delivery channels, employee expertise, employee turnover, testing results, ability to get to root cause of an issue and customer complaints. If there are no gaps, the assessments may not be diving deep enough. Exposed gaps should be risk-weighted and while not all gaps need to be addressed, those that pose a risk of loss or harm need to be documented and formally mitigated. In these situations, all stakeholders should develop an action plan that has measurable benchmarks to determine the success or failure of actions taken.

CMS assessments ask the tough questions and "what-ifs."

There are certain areas to which Institutions should pay special attention:

- **The FCRA** should have a standalone policy, which many institutions don't currently have. It could be advantageous to build this out, including the responsibilities of the business line, product and service.
- **The Vendor** Management Program should be a standalone document as well. It can include the vendor management policy of the institution, but must be detailed enough to guide the institution in how to oversee, monitor, periodically update and terminate a third-party relationship.
- **The privacy** policy should address internal and external causes related to data breaches (identifying the breach; reporting to state agencies, customers and the board; and mitigating reputation risk). It should clearly define what is considered "NPI," the controls to mitigate any risk and what happens if there is a significant breach.
- **The cyber** policy should be a "cyber resiliency policy" that encompasses both the information security and the IT policies. In the past, it was acceptable to combine these two policies; however, because of increasing complexities, standalone policies are now the industry standard.
- **The Bank Secrecy Act/anti-money laundering (BSA/AML)** policy should address incident reporting, which would include internal and external breaches. This is often silent and, due to compliance and BSA reporting, is distributed through different channels of an institution with little interaction.

Procedures for every business line should have a section on data breaches. It is very rare to find business line procedures which provide guidance on what to do if there is a breach; if a customer has been victim of a breach; and how to identify fraud. Institutions might consider expanding certain types of existing business unit procedures (such as identification theft and fraud) that can easily be expanded to include data breaches. A cyber framework should be formalized with a global assessment of the institution.

Institutions should always use three lines of defense for monitoring: The first line is the best defense. They interact with customers and the public. Daily operations should have known trigger points. Impose targeted testing of credit report use, analysis of early defaults, procedures to handle return mail (email and postal) and monitoring of call center calls and email interactions. The second line should test applicable regulations by business line. It has been customary to only test cybersecurity annually through the IT department, but this is not sufficient for the institution as it cannot gauge day-to-day compliance with cyber-risks. Cyber experts must monitor all systems, vendors and sub-vendors. The third line testing should generally be validation of the first and second line oversight with a focus on deep-dive penetration. Any third line reliance on cyber testing should be moved to the second line. System validations may also be done within the second or third lines.

Training should be constant; an annual training schedule is no longer enough. Cybersecurity is inherently high risk and constantly evolves. Institutions should have a method to discuss and evaluate industry issues, enforcement actions and changes both internally and externally. Documentation of the training must remain a high priority. Although there may not be impenetrable defense for data breaches, if the institution can demonstrate efforts in training (e.g., having a multi-faceted, documented training program adequate for inherent risks), this could mitigate potential enforcement actions if a breach were to occur. The board of directors must be educated, at least quarterly if not more frequently. Customized training is ideal, and this can be supported with online training and attendance at industry conferences. The assigned CISO should be involved with developing the training program.

Some Common CMS Weaknesses

Culture does not support a comprehensive CMS. The tone from the top is critical. Management, CEO and the board of directors must understand the risks, support the resources needed to improve the CMS and provide active guidance.

Policies and procedures are vague.

Monitoring does not include all three lines. Testing is not targeted or broad enough, or is completed by those who lack the necessary knowledge. Identified issues are not clearly defined or reported to management, and root cause analysis does not address the actual cause. Validation of remediation is not performed and as a result, there are repeat issues.

Training is not appropriate for the audience (too high-level or not customized). Training fails to include identified issues, best practices and industry challenges.

ROBERT CARDWELL

MANAGING PRINCIPAL
FOCUS ON CONSUMER FINANCE AND FAIR BANKING

"As financial institutions digest the magnitude of the recent breach and its implications for their customers and operations, compliance with the FCRA should be a top-of-list priority. The FCRA imposes strict requirements on furnishers of consumer credit information to the three major credit reporting agencies. As most financial institutions are furnishers, it is imperative that controls around the FCRA'S identity theft requirements be regularly tested and verified. How long ago did you test for FCRA compliance? Was the scope and breadth of the testing adequate? How could you improve it? Were action items addressed and corrective action made? These are just a few of the questions financial institutions should be asking themselves as regulators and consumers apply more scrutiny to this area."

Some common examples of weaknesses found through FCRA testing include:

1. Failure to investigate and respond in a timely manner to consumer disputes of the accuracy and completeness of information reported
2. Failure to conduct end-to-end testing from the source data that resides on the furnisher's system of record all the way through what the agencies report to end users of consumer information reports
3. Consumer reporting agencies' failure to properly place fraud or active-duty alerts on consumers' credit files when requested, and furnishers' and users' failure to properly re-verify the identity of the consumer when notified of a fraud alert before processing a request for new or extended credit
4. Furnishers improperly coding updated information for the consumer reporting agencies via the browser-based, Metro 2 compliant system Online Solution for Complete and Accurate Reporting (e-OSCAR)
5. Not ensuring there is a permissible purpose to pull a credit report

Remedial actions for these weaknesses include:

- Strengthening policies and operating procedures
- Conducting specialized FCRA training
- Increasing the frequency and scope of periodic monitoring and testing
- Documenting the remedial action and steps taken to prevent recurrence

It is important to remember that there is a likelihood of customer harm under FCRA only when personally identifiable NPI is exposed. For instance, if hackers obtain only account numbers without any additional identifying information such as name, social security number, driver's license number, etc., the breach would not raise liability under the FCRA or GLBA. Those considered "furnishers" must always protect the confidentiality of personally identifiable NPI under FCRA, GLBA and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

NON-BINDING GUIDANCE:

ATTEMPTING TO BRING CLARITY TO A CONSTANTLY CHANGING FIELD

While the recent rise in cyberthreats forces financial institutions to rethink many angles of cybersecurity, some regulatory agencies are shifting their focus in the area as well.

CFPB Publishes Guiding Principles

On October 18, 2017, the Consumer Financial Protection Bureau (CFPB) published non-binding principles for safeguarding consumers when they authorize third parties to access their financial data. The principles are intended to "help foster the development of innovative financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives."

The principles relate to any company that requires consumer authorization to access a third party's database. Activities requiring this type of access include fraud screening and identity verification, personal financial management and bill payment. The CFPB based these principles on research it has conducted over the past few years, including feedback from a 2016 Request for Information which garnered responses from industry participants, consumer advocates and individual consumers.

The principles relate to:

- Data access
- Data scope and usability
- Control of the data and informed consent
- Payment authorizations
- Data security
- Transparency on data access rights
- Data accuracy
- Accountability for access and use
- Disputes and resolutions for unauthorized access

Among the other non-binding guidance produced recently is the Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector, which the finance ministers and central bank governors of the G-7 countries released on October 13, 2017. This report advances work released last year and comprises elements of cybersecurity for public and private financial institutions, providing tools for institutions to evaluate the performance and assessment of their cybersecurity practices. It also illustrates a set of outcomes of sound cybersecurity and process components to assist institutions in evaluating their cybersecurity.

In response to this paper, Treasury Secretary Steven Mnuchin commented on the need for such work, and summed up the conflicted feeling many in the financial industry share, by stating:

"Technology has become the global engine driving innovation and economic growth, and it provides a channel for the financial sector to engage customers and counterparties. However, this trend brings increased cyber risk, which is real, dynamic, and evolving."

While institutions strive to protect their businesses and their clients, the new risks demand new security tactics and constant vigilance to protect all aspects of operation and services. It is clear that there are developments on the horizon, and the best way for institutions to stay abreast of the situation is to continue monitoring and updating as constantly as the cyberworld itself.

BENEFICIAL OWNERSHIP RULE AND LESSONS LEARNED FROM THE ACAMS CONFERENCE

At the September 2017 Association of Certified Anti-Money Laundering Specialists (ACAMS) conference, it became clear that financial institutions are expending significant time and resources to the implementation of the Financial Crimes Enforcement Network's (FinCEN) "Beneficial Ownership Rule," which becomes effective in May 2018. With almost a year and a half passed since the rule's issuance, institutions' preparedness currently varies, and compliance with certain portions of the rule is proving to be tricky.

A major discussion point at the ACAMS conference was the "25 percent" condition for the ownership prong of the rule. As we will outline later in this article, many conference participants left with the view that even though the rule requires determination of beneficial ownership for those with 25 percent or more ownership, institutions should probably consider setting a lower percentage threshold for high-risk customers and document their findings.

The beneficial ownership regulation does two things:

1. Extends Customer Due Diligence (CDD) requirements under Bank Secrecy Act (BSA) rules to the natural persons behind a legal entity
2. Adds a fifth pillar to the traditional "four pillars" of an effective anti-money laundering (AML) program by requiring covered financial institutions to establish risk-based procedures for conducting ongoing CDD

The beneficial ownership requirements have been designed to:

- Assist law enforcement in financial investigations
- Help prevent evasion of targeted financial sanctions
- Improve the ability of financial institutions to assess risk
- Facilitate tax compliance and align U.S. compliance with international standards

To comply with the rule taking effect, institutions must include a method of personally identifying each individual who meets either or both of the following criteria for a legal entity client:

- **"Ownership prong"**: owns 25 percent or more of the equity interests in the legal entity customer
- **"Control prong"**: has significant responsibility to control, manage or direct a legal entity customer, including an executive officer or senior manager or any other individual who regularly performs similar functions

A single natural person can meet one of the requirements or both, and a legal entity may have more than one beneficial owner. Logically, under the new rule, there can be up to four individuals who satisfy the ownership prong (i.e., own 25 percent or more of the equity interest). For banks who choose a stricter threshold for ownership determination, there can be more (e.g., up to 10 beneficial owners at 10 percent).

In some cases, a legal entity may not have a beneficial owner under the ownership prong, but institutions are required to identify at least one individual under the control prong. There is no limit on the number of individuals considered beneficial owners under the control prong.

Who is included?

"Covered institutions" under this rule are the same as "covered institutions" under the Customer Identification Program (CIP) — including banks, broker-dealers in securities, mutual funds, futures commission merchants and introducing brokers in commodities.

These covered institutions must perform enhanced due diligence on **"legal entities,"** which are entities created by filing public documents with the secretary of state or similar office, including any similar entity formed under the laws of a foreign jurisdiction. An entity type is generally excluded if it is subject to federal or state regulation, and information regarding its beneficial ownership and management is available from federal or state agencies.

As stated above, while the 25 percent ownership rule requires identification, an institution should consider lowering that threshold if the institution has previously used a lower percentage or has other reason to believe a customer is high-risk.

At the ACAMS conference, a representative from the Federal Reserve Board (FRB) discussed how a financial institution that has classified a customer as "high-risk" and performed enhanced due diligence on that customer, including determining beneficial owners with, for example, 15 percent or 10 percent ownership, should not use the new beneficial ownership as an excuse to relax their policies and procedures. Determining a threshold should be risk-weighted, and if an institution has reason to believe a lower threshold is safer, it is prudent to apply stricter policies than the required 25 percent. At the very least, if an institution decides to keep it at 25 percent, strong documentation should exist explaining every applicable situation, decision and the reasons for that decision.

.

Additional Expectations for Non-required Action regarding Trusts

Another point brought up at the ACAMS conference was whether certain excluded legal entities should always be excluded. Specifically, some regulators claimed that for trusts, it may be prudent in certain situations to collect information when not technically required. Since most trusts do not need to file public documents upon establishment, FinCEN has noted that "identifying a 'beneficial owner' from among" trust grantors, trustees and beneficiaries "would not be possible."

However, FinCEN does recommend that an institution obtain some information on trust accounts' beneficial owners in some instances: "We reiterate our understanding that, consistent with existing obligations, financial institutions are already taking a risk-based approach to collecting information with respect to various persons associated with trusts in order to know their customer, and that we expect financial institutions to continue these practices as part of their overall efforts to safeguard against money laundering and terrorist financing."

And, of note, when a trust is a beneficial owner of a legal entity customer, the trustee of the trust is to be considered the "beneficial owner."

Key Requirements

Once a beneficial owner is identified, a covered financial institution must do the following to comply with the rule:

- Obtain the name, address, date of birth and social security number for every beneficial owner
- Verify the above information according to the financial institution's CIP
- Understand the nature and purpose of the customer relationships
- Create a customer risk profile using information gathered at account opening and include in enhanced due diligence reviews of the entity
- Conduct ongoing monitoring
- Update beneficial ownership information whenever monitoring reveals that a change in ownership has taken place
- Retain identification records for five years after the account is closed and verification records for five years after the record is made

Two Interesting Aspects of the Rule

1. Covered institutions may rely on other financial institutions to perform the requirements to identify beneficial ownership, provided that the covered institution has no knowledge of facts that would reasonably call into question the reliability of the information.

   For this to hold true, institutions must follow CIP reliance requirements (i.e., having a signed agreement between the financial institution and whomever is performing CIP and annual certification).

2. CDD information can be monitored and updated on an event-driven basis rather than an ongoing basis

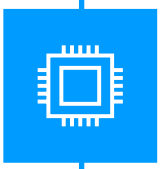
Regulatory Resources

Fed Register Document Number 2016-10567

The rules contain CDD requirements and included a new requirement to identify and verify the identity of beneficial owners of legal entity customers. This rule became effective in July 2016.

FIN-2010-G001

The FAQs detail CDD requirements for financial institutions. FinCEN defined obtaining beneficial ownership information as necessary to meet an institution's "comprehensive" CDD responsibilities, particularly related to "high risk customers."



Interagency Guidance

This document offers guidance on beneficial ownership from the banking industry, federal agencies and examination staff. The revisions clarify supervisory expectations and incorporate regulatory changes since the manual's 2010 update.

Appendix K

Appendix K addresses customer risk versus due diligence and suspicious activity. This information aids in properly assessing a customer's risk profile.

How the Rule may Affect AML Compliance for CTRs

While the cash transaction report (CTR) aggregation rules are not changing, the CTR process may change. If an institution has knowledge that the same person conducted multiple transactions, the institution must aggregate these transactions for CTR filing purposes. With the new beneficial ownership rule, an institution may realize certain transactions that would not have been aggregated before are now subject to aggregation, because there is more clarity as to who is behind transactions on behalf ofan entity.

Some Final Thoughts

BSA/AML compliance continues to be among the most important and visible issues for financial institutions. The scope of CDD for BSA/AML compliance is widening, and it is necessary for institutions to create a more comprehensive approach to regulatory monitoring and compliance in order to preserve safety and soundness, mitigate illegal activity and avoid penalties and costs to rectify non-compliance.

To achieve these goals, it might be prudent to: revamp your institution's CDD policies, procedures and process; collaborate with the core system processes and AML software; budget for additional staff for CDD maintenance; and risk rate your customer base on an ongoing basis.

ABOUT CAPCO

Capco is a global business and technology consultancy dedicated to the financial services industry, plus a dedicated energy division. Capco delivers innovative solutions in Banking & Payments, Capital Markets, and Wealth & Asset Management, designed to withstand market forces, continual regulatory change and increasing consumer demand.

WORLDWIDE OFFICES

Bangalore	Hong Kong	Singapore
Bratislava	Houston	Stockholm
Brussels	Kuala Lumpur	Toronto
Chicago	London	Vienna
Dallas	New York	Warsaw
Dusseldorf	Orlando	Washington, DC
Edinburgh	Paris	Zurich
Frankfurt	Pune	
Geneva	São Paulo	

CONTACT US

Capco Center of Regularoty Intelligence
1101 Pennsylvania Ave.,
NW Suite 300 Washington, DC 20004
E: capco.cri@capco.com
P: 202.756.2263

@CAPCO

WWW.CAPCO.COM

CAPCO