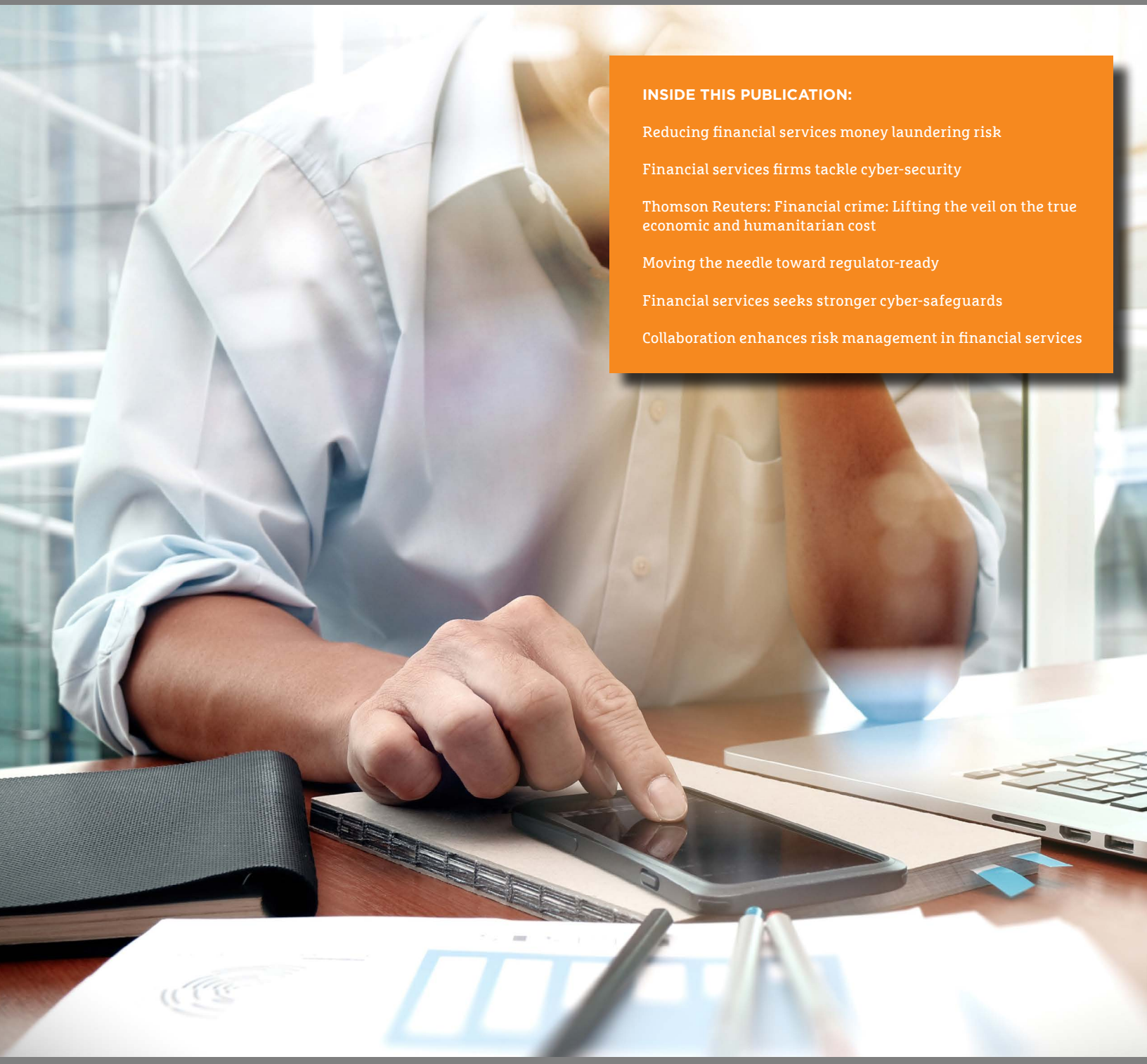
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Reducing risk in the **Financial services industry**

An e-Book publication sponsored by THOMSON REUTERS™

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

THOMSON REUTERS™

Risk Management Solutions from Thomson Reuters combine what no one else can—trusted information, managed services and software, and human expertise—to help you manage risk efficiently and accelerate business performance. With this combination, you can confidently anticipate and act on customer, third party, compliance, enterprise, and financial risk while you elevate corporate governance and controls across your organization.

Most jurisdictions and regulatory regimes concerned with combating fraud and financial crime have legislation which makes it mandatory for regulated industries to have procedures in place to curtail money laundering activities. Failure to report such illegal activities can result in regulatory censure, financial penalties, reputational damage as well as being subjected to ongoing monitoring by regulatory authorities.

At Thomson Reuters, we understand to Know Your Customer is a serious business and compliance is not simply an option, or just a 'nice to have." The mandate to know who you are doing business with and to ensure those parties are operating in a lawful and compliant manner, is more urgent, more tightly regulated and more complex than ever before. Both financial institutions and corporate organizations want to spend more time running their businesses and less time on KYC.

We deliver market-leading risk management solutions for global regulatory intelligence, AML, KYC, financial crime, anti-bribery and corruption, supply chain risk, enhanced due diligence, and enterprise governance, risk and compliance management. Thomson Reuters provides customer identification solutions for any market or organization—as well as capabilities for client on-boarding, screening software, enhanced due diligence and transaction monitoring—leveraging leading products such as World-Check. Visit https://risk.thomsonreuters.com.

Inside this e-Book

Reducing financial services money laundering risk

Thanks to two recent reports, risk and compliance professionals in the financial services industry can take the pulse of their BSA/AML compliance programs and better understand how they stack up against their peers. **Jaclyn Jaeger** reports.

Amid intensified regulatory scrutiny and enforcement in the financial services industry, prudent risk and compliance professionals in banks of all sizes will want to check out two reports that will help them gauge the effectiveness of their Bank Secrecy Act compliance programs.

The Bank Secrecy Act (BSA) refers to a series of laws and regulations that have been enacted in the United States to combat money laundering and terrorism financing. By law, financial institutions must monitor for suspicious activities and identify and report them to law enforcement.

To assess the current state of BSA compliance programs, the Federal Deposit Insurance Corporation (FDIC) has issued a Supervisory Update that provides an overview of the BSA/Anti-Money Laundering (AML) examination process, discusses trends in supervision and enforcement, and includes examples of rare, but significant, failures identified by FDIC examiners in BSA/AML compliance programs.

Secondly, RSM, a provider of audit, tax, and consulting services, conducted a benchmark report in which it assessed the BSA/AML compliance departments of over 100 U.S.-based commercial banks nationwide, ranging between $500 million to $20 billion in assets. The results were based on the responses of 132 senior-level officers and managers responsible for oversight of the BSA program at their respective institutions. The survey assessed several key areas, including AML functional structures, budgets, risk tolerance, staffing levels and certifications, training, and technology investments.

Examined together, both the FDIC report and RSM's benchmark report help risk and compliance professionals take the pulse of their BSA/AML com-

pliance programs and how they stack up against their peers—not to mention how they are perceived in the eyes of financial regulatory agencies.

For example, in RSM's benchmark report, 95 percent of respondents said they are generally "satisfied" with the effectiveness of their BSA/AML function, as well as the quality of the risk assessments that drive their BSA compliance programs.

This sentiment appears to be supported by the FDIC's findings. "In the vast majority of examinations, the FDIC finds that institutions generally comply with the BSA," the FDIC said in its Supervisory Update. "When examiners find BSA compliance deficiencies, they are often technical recordkeeping or reporting matters that can be addressed in the normal course of business."

The FDIC report went on to say that common violations of BSA regulations cited during the FDIC's BSA/AML examinations relate to currency transaction report filings and information-sharing requirements. Many of these violations "relate to suspicious activity report filing deficiencies and inadequate systems of internal controls," the FDIC stated.

The Supervisory Update explains how banks can prevent such commonplace violations. "For example, information-sharing compliance deficiencies may be corrected by designating persons responsible for conducting searches, keeping contact information up-to-date with FinCEN, and establishing policies, procedures, and processes that clearly outline methods for conducting and documenting information-sharing request searches, as well as reporting the results of those searches, as necessary."

Compliance staffing and outsourcing. In the RSM survey, 53 percent of respondents said their financial institution has an AML officer or director function. Other commonly cited roles with AML responsibility included a compliance officer or chief risk officer.

RSM's report also found that 76 percent of large banks have at least one certified AML professional, compared to 54 percent of small banks. Additionally, 48 percent of large banks said they employ a certified fraud professional, compared to 26 percent of small banks. And nearly all, except for one percent, have a centralized BSA/AML department.

Many banks, however, appear to have a limited number of staff who are fully dedicated to BSA/AML compliance. The RSM survey found, for example, that 70 percent of respondents said they have five or fewer full-time employees (FTEs) dedicated to BSA/AML compliance. Forty-two percent have fewer than three FTEs; 29 percent have between three and five; and 13 percent have between six and ten FTEs.

Small banks generally have less than half the number of FTEs responsible for BSA/AML compliance compared to large banks. Specifically, 87 percent of small banks have fewer than five FTEs, compared to 53 percent of large banks. And 70 percent of respondents said they do not foresee adding more FTEs in the next year.

Many times, financial institutions turn to outside resources to both increase efficiencies and leverage skillsets that they don't have internally—in particular, BSA/AML internal audits (62 percent) and AML model validation testing (53 percent).

"Typically, for model validation the technical expertise is one that is hard to come by. Therefore, it's extremely expensive and significantly time consuming to acquire that talent to bring in-house," says Patricio Perez, partner and Southeast financial institutions leader at RSM. "It's extremely important for banks to understand that there is a solution out there in outsourcing these kinds of activities."

By bank size, 65 percent of large banks outsourced BSA/AML internal audits, compared to 59 percent of small banks. Furthermore, 58 percent of larger banks outsourced AML model verification testing, compared to 48 percent of small banks.

Other activities that banks sometimes outsource, as cited by respondents, include quality control reviews (8 percent); AML risk assessments (5 percent); and regulation interpretations (2 percent).

Training programs and investments. Ongoing training is a regulatory requirement for BSA/

Cease and desist

Below, the Federal Deposit Insurance Corp. details what warrants a cease and desist order.

To be considered a problem within the meaning of Section 8(s), a deficiency would generally involve a serious defect in one or more of the required BSA compliance program components, and would have been identified in a report of examination or other written supervisory communication as requiring communication to the institution's board of directors or senior management as a matter that must be corrected.

The FDIC does not ordinarily issue a cease and desist order under Section 8(s) unless the deficiencies identified during a subsequent examination or visitation are substantially the same as those previously reported to the institution.

For example:

During an examination, the institution's system of internal controls was considered inadequate as a result of compliance failures related to customer due diligence and suspicious activity monitoring processes. Specifically, the institution had not developed customer risk profiles to identify, monitor, and report suspicious activities related to the institution's business customers.

Additionally, the institution had not implemented an effective system to identify, research, and report suspicious activity. Notably, there was a significant number of suspicious activity monitoring system alerts that had not been properly researched and resolved.

Apparent violations were cited as a result of the institution's inadequate system of internal controls and numerous instances where the institution failed to meet suspicious activity reporting requirements.

The report of examination identified a problem with the internal controls component of the institution's BSA compliance program, which required board attention and management's correction. The issue was explained in the report of examination, which was reviewed by the institution's senior management and board of directors. After the examination, an informal enforcement action was issued to address the problem.

Subsequent examination findings determined that management had not satisfactorily addressed the previously reported problem with its BSA compliance program. Customer risk profiles remained undeveloped for the institution's business customers and suspicious activity identification, monitoring, and reporting processes remained inadequate.

The number of outstanding suspicious activity monitoring system alerts had increased substantially, resulting in additional instances where the institution failed to meet suspicious activity reporting requirements.

As a result, a cease and desist order was issued pursuant to Section 8(s) of the FDIC Act because of the institution's failure to correct the previously identified problem with its BSA compliance program.

AML compliance to keep up with a rapidly evolving regulatory risk environment. As the FDIC Supervisory Update states, compliance deficiencies related to suspicious activity reporting can be prevented with trained staff and by implementing systems to identify, research, and report unusual activity. "Training and systems should be commensurate with an institution's overall risk profile and include effective decision-making processes," the FDIC stated.

In the RSM survey, 94 percent of respondents said their banks use Web-based BSA/AML training for employees, while 68 percent perform in-person BSA/AML training, and 43 percent leverage external training and seminars. "Regulators expect employees to stay abreast of trends and threats, and external training can provide a new perspective on risks," the RSM report stated.

Furthermore, banks should tailor their training to the specific functions of the employee. "The more sophisticated institutions tend to have a more tailored approach to the training," Perez says.

Training budgets may also need to be adjusted. RSM's survey data showed that the median annual budget for BSA/ AML training is $5,000. Twenty-six percent of respondents spend between $5,000-$10,000 per year, while 19 percent spend between $10,000-$20,000, and another 19 percent have a budget between $1,000-$2,000.

When it comes to BSA/AML training budgets, 70 percent think their budget will stay the same, while 29 percent of large-bank respondents said they expect a training budget increase in the coming year. Among small financial institutions, 86 percent expect a stagnant training budget, while 12 percent projected an increase.

Due diligence and suspicious activity reports. RSM's report found that banks file an average of 16.3 suspicious activity reports a month, with 118.6 complete investigations, 39.5 complete due diligence reviews, and 2.7 model or system validations.

"Effective decision-making processes should be supported by adequate documentation regarding decisions to file or not to file a suspicious activity report (SAR)," the FDIC stated. "Because SAR decision-making requires review, analysis, and judgment of transactions, institutions should maintain effective internal control systems that establish appropriate policies, procedures, and processes for suspicious activity monitoring and reporting."

Most large banks (96 percent) leverage technology to identify suspicious activity, compared to 77 percent of small banks, the RSM report found. It also found that the median annual budget for suspicious activity monitoring software was $30,000, followed by case management ($20,000); customer risk scoring ($19,000); and SAR reporting ($18,000).

The good news, overall, as stated by the FDIC: "Most BSA compliance program deficiencies are corrected during the normal course of the supervisory process without the need for a formal enforcement action." And this is important, given that BSA/AML compliance programs play an integral role in deterring and detecting bad actors who seek to misuse the U.S. financial system to launder criminal proceeds, finance terrorist acts, or move funds for other illicit purposes.

Beyond just providing benefits externally to financial institutions, however, a robust BSA/AML compliance program fosters improvements in other areas, as well. For example, RSM's analysis found that 85 percent of respondents expressed overall satisfaction with the extent of their board of director's involvement in their BSA/AML compliance function.

"Board involvement in community banking … has evolved," Perez says. Fifteen years ago, many board members did not understand or pay attention to BSA/AML compliance, he says, but emerging risks like terrorist financing and increased regulatory enforcement have brought with it heighted scrutiny, including board oversight.

With the BSA/AML regulatory environment for financial institutions as fluid as it is, greater involvement by the board of directors should be a welcome development, translating into more effective and efficient oversight moving forward. ■

Financial services firms tackle cyber-security

There is no single solution to prevent the many flavors of cyber-crime. Private enterprise and the government, however, should do a better job of working together, writes **Joe Mont**.

We all know that cyber-security is a scourge in the financial services industry. What, however, are these firms doing about it?

In November 2017 a sub-committee of the House Financial Services Committee held a hearing to examine cyber-security gaps and identify where state and federal data security regulation could be improved.

"More than 15 million Americans were victims of cyber-fraud or identify theft last year," said Sub-committee Chairman Blaine Luetkemeyer (R-Mo.). "While data security has been a hot topic since the latest breach, Equifax isn't where the problem started and, if we don't act, it isn't where the problem will end. With each attack more dangerous and more advanced than the last, it is crucial that every aspect of data security is examined."

The hearing, he said after its conclusion, "reiterated that we need to work collaboratively to reduce red tape, create a prompt notification standard, and foster harmonization among federal and state agencies charged with data security regulation."

He promised that data security reform legislation would emerge in the near future.

"The cyber-security landscape is complex with a wide array of hostile actors, including criminals seeking financial gain, nation states engaged in corporate espionage or worse, and terrorist groups seeking to disrupt markets and create fear," said Kenneth Bentsen, president and CEO of the Securities Industry and Financial Markets Association. "Cyber-crime is now a bigger criminal enterprise than the global narcotics trade."

The financial services industry, he said, is a top target facing tens of thousands of attacks each day. "In simple terms: Financial institutions shouldn't have to devote limited resources to redundant regulatory and supervisory requirements at the expense of actual security-based activities. It is critical that we establish a robust partnership between industry and government to mitigate cyber-threats and their impact."

Working with its members, along with our sister trade associations, SIFMA has recognized a number of best practices for the protection of sensitive data in the financial services sector," Bentsen testified. These practices draw on the experience of our member firms and their own policies and procedures, as well as industry standards such as the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cyber-Security.

Data protection "begins with firms taking a risk-based look at what information they collect," he added. Do they have a business or regulatory purpose that requires them to hold this information? If sensitive information like Social Security Numbers is not directly relevant and necessary, firms should refrain from collecting it.

"Once firms have collected sensitive data, they should ensure that they have controls in place to protect it while it is being used or stored," Bentsen said. This includes ensuring access to sensitive data including investor information is restricted to authorized users who need it to perform their jobs and making sure that as individuals change their roles, their access to sensitive information is updated as well.

"Keeping access to this data focused only for those who need to use it helps reduce the potential points of risk," he added. "Firms should also have policies such as data loss prevention controls and multifactor authentication to control access to sensitive data, as well as maintain a detailed audit trail of how sensitive data is handled while in possession to identify any weaknesses or vulnerabilities."

Bentsen reminded the panel that the focus on data protection also extends "beyond securities firms themselves to encompass other entities with whom we share information." The risks posed by third parties have been recognized by regulators in the United States and internationally, such as the Office of the Comptroller of the Currency's release on third-party relationships and risk management guidance.

Consolidated Audit Trail. Turning to the Securities and Exchange Commission's plans for a Consolidated Audit Trail (CAT), Bentsen said that his member firms want to ensure that the development of the CAT "does not introduce new data protection risks."

Once complete, the CAT will be the world's largest data repository for securities transactions and one of the world largest databases of any type. Every day the system would ingest 58 billion records (orders, executions, and quotes for the equities and options markets) and would maintain data on over 100 million customer accounts and their unique customer information. This data would grow to an estimated 21 petabytes within five years, the equivalent of over ten times the content of all U.S. academic research libraries, in a single database.

"As currently designed, the CAT could also be a gateway for cyber-criminals to access confidential trading information and the personal information of tens of millions of retail investors," he said. "The current CAT plan requires reporting firms to provide a significant amount of sensitive customer information, including name, SSN, and address. It will also hold sensitive trade information, which could be used to reconstruct proprietary trading strategies ... This information will be held in a single database that creates a high value target, and bad actors will have a strong incentive to find the weakest link to gain access."

"While our concern existed before the recent breaches, many stakeholders remain skeptical that the CAT, as currently designed, will be able to protect the massive amount of sensitive PII for every investor in America," he added. "Despite serious data protection concerns, the CAT technical specifications that have been released to date include alarmingly few details on data security and protection."

Bentsen stressed collaboration. In recognition of the cyber-threat to the financial sector, a coalition of financial services trade associations and the Financial Services Sector Coordinating Council, working with

SROs, state regulatory agencies, and members of the Financial and Banking Information Infrastructure Committee agreed to create forums to discuss various guidance, tools, frameworks, regulations, and examination processes, built around the NIST Framework.

Daniel Mennenoh, president of the H.B. Wilkinson Title Co., an Illinois-based title insurance agency, testified that cyber-security is not a problem the industry can fix on its own. "What is so frustrating is that there is no amount of money we can spend to protect our consumers from being targeted by these criminals," Mennenoh said. "Probably the single biggest preventative measure that real estate and banking professionals can take is to encourage consumers to call the title company or real estate agent to verify wire instructions before transmitting funds," he added.

He also urged firms to match not only the account number of the recipient but also the payee's name. Often the fraudulent instructions will say the transfer is to be sent to the title company's trust account, but instead it goes to the criminal's personal account.

"Just matching the account number on the request with an account number at the beneficiary bank will not catch this," he said. "Some banks have voluntarily added capabilities to match the payee's names, and it is proving useful in catching these schemes."

Edmund Mierzwinski, U.S. PIRG's consumer program director, cautioned Congress not to move forward on any data security legislation "that would preempt strong state privacy leadership or would endorse closed or non-technology neutral standards."

"Federal law should never become a ceiling of protection; it should always serve as a minimal floor that allows state experimentation," he said. "[It] should not endorse specific solutions that limit innovation."

The United States, Mierzwinski suggested, should move beyond the "sectoral approach" embodied in the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act.

The FCRA, for example limits the use of consumer credit reports only to firms with certain permissible purposes (generally, determinations of a consumer's eligibility for credit, insurance, and employment); it requires credit bureaus (data collectors) to meet certain accuracy standards, and it allows consumers to review their files, dispute, and demand corrections of mistakes and to control the secondary use of their files by opting out of marketing uses of their reports.

The U.S. sectoral-only privacy laws should be contrasted with the new European General Data Protection Regulation, he said. It provides over-arching privacy rights to European citizens over corporate usage of their information, including rights to control the use of their information and to seek redress (and compensation) against the infringing company.

"Importantly, the GDPR ... trumps the existing Privacy Shield applicable to U.S. firms doing business in Europe and provides a roadmap for U.S. companies to improve their treatment of U.S. consumers," he testified. "In particular, since SIFMA member firms will be subject to the GDPR, it seems that they can import those protections to small investors in the U.S., rather than seek, as they may today, to weaken applicability of existing state data security and identity theft laws."

That being said, Mierzwinski stressed that Congress needs to allow customers to hold firms more accountable—such as by way of civil litigation.

"Data security, ensuring member safety, and how to incentivize and emphasize Congress must ad-dress data security issues and "move forward with meaningful legislation that will make a difference to consumers," said Debra Schwartz, president and CEO of Mission Federal Credit Union on behalf of the National Association of Federally Insured Credit Unions.

Credit unions and other depository institutions already protect data consistent with the provisions of the 1999 Gramm-Leach-Bliley Act and are examined by a regulator for compliance with these standards.

"Unfortunately, there is no comprehensive regulatory structure similar to what GLBA put in place for depository institutions for other entities that may handle sensitive personal and financial data," Schwartz said. "Too often, credit unions are left cleaning up the mess and helping their members restore their personal financial information after another entity has suffered a breach." ■

EXPERT TALK

FINANCIAL CRIME: LIFTING THE VEIL ON THE TRUE ECONOMIC AND HUMANITARIAN COST

By Che Sidanius

The true cost of financial crime extends far beyond pure economics. Critical social and humanitarian consequences impact the lives of millions of individuals across the globe on a daily basis. When viewed in its entirety, can we ever really quantify the cost of this so-called 'victimless' crime?

"Financial crime causes incalculable harm around the world. The proceeds of bribery, corruption, fraud, narcotics trafficking and other organized crime have all been implicated in the financing of terrorism, human rights abuses such as slavery and child labor, and environmental crime. This has serious economic and social costs in terms of the lost revenues to national exchequers that could be invested in social development, and in terms of the impact on individual lives."

Che Sidanius, Global Head Financial Crime Regulation & Industry Affairs, Thomson Reuters

ON-THE-GROUND INSIGHTS

As part of our ongoing commitment to exposing the true cost of financial crime, Thomson Reuters commissioned a global survey during March 2018 and collated insights on this type of crime from over 2300 senior managers of large organizations, both publicly listed and privately owned, across 19 countries[1]. In order to build a more complete picture of the social and financial impact of financial crime, we broadened the scope to include bribery and corruption; money laundering; fraud; theft; cybercrime; and slave labor/human trafficking.[2] Survey results were further supplemented by conducting in-depth interviews with leading NGOs (Education Endowment Foundation, Transparency International UK and Walk Free Foundation) and the European Union's law enforcement agency to gain perspective on the humanitarian cost and implications of this pervasive form of crime.

BACKGROUND TO THE CHALLENGE

Before delving into the impact of different types of financial crime, our survey uncovered some of the factors that have created an ideal environment for these crimes to continue:

- ***Extensive networks***
  Survey results revealed that one in 10 organizations had dealt with over 10 000 third party vendors, suppliers or partners during the preceding 12 months and the global average number of such relationships was reported as 7 693.

- ***Inadequate screening***
  Whilst screening, both at the initial onboarding stage and on an ongoing basis, can never hope to completely eradicate financial crime, it is nonetheless recognized as an important tool to identify potential links to crime. Survey results revealed that an average of just 59% of these third party vendors, suppliers or partners were screened at onboarding and the same percentage are monitored and reviewed on at least an annual basis. This means that only approximately 35% of all relationships are fully screened.

- ***Lack of reporting***
  59% of all detected financial crime is reported internally and, for the most part, reported externally.

- ***Ever-increasing pressure***
  Organizations are under ever-increasing pressure: 83% of survey participants expected that pressure to increase turnover would be either extreme or significant in the 12 months post-survey.

This combination of factors – extensive third party networks and insufficient screening and reporting, against a backdrop of increasing pressure to grow profits – has led to a situation where financial crime is flourishing across the globe.

THE TRUE IMPACT: FINANCIAL AND HUMANITARIAN

Financial crime is pervasive, with 47% of organizations confirming that they had been the victim of such crime in the year preceding the survey. Public companies appear to suffer more – 55% of publicly listed companies said that they had experienced some form of financial crime in their global operations over this period, against 45% for private companies. The estimated total loss as a result of

these financial crimes is USD1.45 trillion, equating to 3.5% of annual turnover.

Many people assume that financial crime impacts big business alone and it is therefore often regarded as 'victimless', but nothing could be further from the truth. The human cost of financial crime is also significant. The Global Slavery Index, produced by the Walk Free Foundation and International Labour Organisation, estimates that 40.3 million people today are in modern slavery, with just five countries – India, China, Pakistan, Bangladesh, and Uzbekistan – responsible for 58% of this total. The cost of slavery/human trafficking in the EU is estimated to be €30 billion, and extrapolating this on the dual assumptions that the EU represents approximately 20% of the global economy, and that other areas of the world have a similar prevalence, this puts the global cost at €150 billion, broken down as follows:

- USD99 billion from commercial sexual exploitation
- USD34 billion in construction, manufacturing, mining and utilities
- USD9 billion in agriculture, including forestry and fishing
- USD8 billion dollars is saved annually by private households that employ domestic workers under conditions of forced labor

> *"Ordinary people everywhere in the world unwittingly meet victims of modern slavery every day – we might walk past a young woman trapped in a forced marriage, a hotel cleaner that has had her passport confiscated, or touch this crime through clothes we wear that were made through illegal forced labor."*
>
> **Fiona David, Executive Director of Global Research, Walk Free Foundation**

There are a host of further examples of financial crime impacting individual lives, such as lost tax revenue that could have funded essential services like education. When these funds do not reach the coffers of national exchequers, a vacuum is created. By way of example, The Education Endowment Foundation calculates that every USD1bn in missing tax revenue equates to:

- High-quality early years education for 150,000 toddlers in Spain.
- Places for 327,000 children in primary and secondary schools in Mexico.
- Approximately 2,000 more schools in India.

Examples such as these merely hint at the total societal and humanitarian cost born by millions of individuals across the globe every day.

THE CURRENT STATE OF PLAY

Compliance and training gaps

Organizations are largely aware of the incidence of financial crime and are hardly resting on their laurels. Respondents estimated that they spent an average of 3.1% of turnover to prevent these issues occurring around their global operations – a collective spend of USD1.28 trillion – in the past year. Despite this, inefficiencies and significant gaps in formal compliance procedures remain: respondents globally revealed that just 57% fully screen and classify risk; 52% fully conduct due diligence; and 52% fully monitor and refresh records.

Gaps in training are also evident. By way of example, just 46% of respondents confirmed that formal training is undertaken by colleagues around the globe in identifying, preventing and reporting breaches in slave labor/human trafficking.

A lack of data intelligence

Rob Wainwright, former Executive Director, Europol says that his organization estimates that barely 1% of criminal proceeds generated in the European Union are confiscated by relevant authorities, despite the fact that global banks spend billions of dollars each year meeting stringent anti-money laundering regulations. This suggests that current regulatory regimes are highly inefficient.

Europol research further shows that, over a period stretching back to 2006, an average of only 10% of all suspicious transaction reports received by law enforcement agencies across Europe ever led to any meaningful investigation, with a primary reason identified as 'the general paucity of good-quality intelligence delivered by the system'.

WHAT CAN BE DONE?

When it comes to rooting out financial crime, reliable and complete data, as well as industry-wide collaboration are important tools in this ongoing fight.

Data is a critical requirement needed to develop a 360 degree view of risk. Only when this 'paucity of intelligence' has been remedied can organizations hope to plug the identified compliance gaps. When selecting a financial crime data partner, advanced technological capabilities are a valuable area for companies: 66% saying they have this already and 31% are considering it. Approximately half of respondents cite the importance of subject matter expertise, research methodology and breadth and depth of information.

Globally, 94% of respondents are supportive of sharing financial intelligence/information on specific cases and sharing compliance best practice, pointing to a clear appreciation of the importance of collaboration in the fight against financial crime. To this end, new collaborations are already being formed, as David Craig, President

Financial & Risk, Thomson Reuters, elaborates, 'at Davos 2018, the World Economic Forum, Thomson Reuters and Europol launched a coalition to improve awareness of the extent of financial crime, promote more effective information sharing and establish enhanced processes to share best practice.'

Undoubtedly the first step to thwarting financial criminals is to unveil and raise awareness of the full impact – both economic and humanitarian – of this pervasive global scourge. Ongoing initiatives to root out financial crime at all levels are encouraging, and are further supported by recent IMF (International Monetary Fund) initiatives in this space: in April 2018, the IMF announced that its Executive Board had just endorsed a new framework for stepping up engagement on governance and corruption in member countries, commenting that, 'to be truly effective, anti-corruption strategies… require broader regulatory and institutional reforms. At the end of the day, the most durable 'cure' for corruption is strong, transparent, and accountable institutions.'[3]

Thomson Reuters, as a critical partner in the fight against financial crime and a source of trusted answers, helps customers anticipate, mitigate and act on risk with confidence.

---

1 The individual countries included in the survey were: The USA, Canada, China, India, Singapore, Australia, the UK, Germany, the Netherlands, Spain, France, Russia, Poland, the UAE, Saudi Arabia, South Africa, Nigeria, Brazil, Mexico.

2 Please note that the standard convention of rounding has been applied and consequently some totals do not add up to 100%.

3 https://blogs.imf.org/2018/04/22/shining-a-bright-light-into-the-dark-corners-of-weak-governance-and-corruption/

AUTHOR BIO:

Che Sidanius

Che is the Global Head of Financial Regulatory & Industry Affairs. His role is to manage how regulatory changes around financial crime affect Thomson Reuters Risk & Supply business globally. His responsibilities include proposing courses of action to address regulatory changes and drive execution throughout the organizations. His previous experiences include working at Big 4 consultancies within Capital Markets Advisory, as a Senior Advisor at the Bank of England, and a Senior Examiner at the Federal Reserve Bank of New York during the 2007-09 financial crisis.

Moving the needle toward regulator-ready

Employing centralized data processing is a capability that many firms simply cannot afford to live without. **Roy Kirby** has more.

Once upon a time, when financial institutions had to comply with a new regulation, they would create a dedicated team to deal with each specific regulation. This group of compliance professionals would oversee the process from start to finish, acquiring data, parsing it for information needed, and assembling the necessary reports and conclusions to relay to the regulating authorities. Every time a rule was passed down from regulators, the process would begin anew, leading to a world where compliance departments were a complex mix of siloed teams, each working on its own to carry out a particular section of the regulatory agenda. Each firm would have a faction for FATCA, a division for Dodd-Frank, a squad for sanctions, and so on.

When banks had only a few distinct regulations to worry about, this approach may have made sense, and it's easy to see how it has continued to endure over the years as new rules slowly trickled out in piecemeal faction. Today's regulations, though, are more complicated and intertwined than ever before. As the pace of rulemaking has picked up, the complex and overlapping directives that have resulted are beginning to look like a plate of regulatory spaghetti. Banks are facing a raft of regulations that draw from nearly every conceivable corner of their

data resources. These regulations contain some of the most extensive reporting requirements ever, mandating that firms provide data on trading venues, client order volumes, liquidity, and trade execution, among other things. They also require qualitative information showing that firms are adhering to best execution requirements in their trading procedures. Compliance managers know that regulators will be examining their programs closely and looking for errors or omissions that may be indicative of a larger problem and can set a firm up for additional scrutiny. Even firms' compliance must be compliant, and to show that they're making a good-faith effort in this regard, they need procedures that are organized and efficient, making it easier for them to diagnose, correct, and ultimately avoid mistakes.

In this environment, traditional siloed approaches seem quaintly outdated at best and dangerously inefficient at worst. To comply with each of the current slate of regulations, firms need to access massive streams of data, pulling the correct data and applying the appropriate rulesets. Yet, when a siloed approach is used, multiple teams often end up accessing the same data on their own—a situation that not only leads to data redundancy and duplication, data sourcing complexity and convoluted time series management, but can potentially also cause serious issues in the event of data discrepancies.

Imagine if any time you wanted to watch a new movie you had to subscribe to a new streaming service, or if you wanted to listen to a new song you had to download a new music application. Not only would the effort required to take these extra steps build up to mind-numbing proportions, but the end result would be a chaotic hodgepodge of software, data, and expenses. If banks do not rethink the way they're utilizing financial data in today's regulatory landscape, this could be the scenario for which they are headed.

Complying with even one complex new regulation—such as the rapidly approaching MiFID II—and proving to regulating authorities that proper reporting standards are being met is going to require a small army of compliance, software, IT, finance, and administrative staff. With new amendments and changes to these regulations almost certain to continue emerging, firms are coming to the realization that a full-scale rethink of how they do things is required. The silos that have defined compliance teams since the beginning are going to have to come down and more innovative solutions are going to have to take their place.

With so much legwork to do, and so much data to delve through, firms will need to streamline their approaches, taking advantage of the overlapping data sets that major regulations all require. Instead of piling on to their mountains of statistics, compliance staffs are looking to implement standardized, scalable services that will allow them to easily compile and extract the quality reference data they need, packaged up in the way they need it. This will enable them to unravel their regulatory spaghetti by using the common services shared by various regulations.

The data analysis burden necessary for complying with regulations is quickly becoming more than old-school compliance teams can bear. In order to untangle the knot of requirements, firms are going to have to rethink their processes and take advantage of what today's innovative data service technology has to offer. Compliance teams are already stretched thin, and they risk major, reputation-damaging errors if they devote their time to tiresome, complex, and redundant data extraction tasks that could be done automatically. They need structured data flows that do the grunt work of mapping things out and allow them to focus on the hard work of creating an effective compliance environment.

The increasing complexity of the financial landscape has undoubtedly made life more difficult for compliance teams than it was in the good old days, but major advancements in data technology are helping them to keep pace and maintain their balance. Those firms that take advantage of these innovations to consolidate their compliance approaches will be able operate with confidence. Those that do not are likely to get left behind. ■

Roy Kirby is Senior Product Manager for SIX Financial Information.

Financial services seeks stronger cyber-safeguards

A rising tide of sophisticated cyber-thievery has the financial services industry scrambling to improve its electronic defenses. But can they find a solution before the next big heist? **Jaclyn Jaeger** has more.

In February 2016, cyber-thieves stole $81 million from the Central Bank of Bangladesh by sending fraudulent messages through the SWIFT payment network. The heist sounded a wake-up call that if financial services firms wanted to protect themselves against similar acts of thievery, they would have to evolve their defenses, and quickly.

First, some background. SWIFT is short for the Society for Worldwide Interbank Financial Telecommunication, a global industry cooperative. More than 11,000 financial institutions in more than 200 countries and territories around the world use SWIFT's messaging platform, averaging some 26 million SWIFT messages per day, and more than six billion in 2016, according to SWIFT figures.

The Bank of Bangladesh attack opened a Pandora's Box, as criminal groups ramped up copycat attacks. SWIFT stopped short of disclosing the number of attacks, identifying the banks involved or disclosing how much money was stolen, but details of some of these attacks have become public. Far Eastern International Bank, for example, lost $500,000 in a cyber-heist, believed to have been launched by a North Korean Lazarus hacking group, suspected to be the same hacking group behind the Bangladesh heist. In another reported attack, Nepal's NIC Asia Bank lost $580,000 in a cyber-heist in November 2017.

In all these attacks, security weaknesses in the compromised banks enabled cyber-thieves to gain administrator access to the banks' payment environments, according to the SWIFT report. With this access, hackers not only stealthily monitored the banks' operations—sometimes for months—but also were able to modify security defenses and the operation of software to enable their attacks by updating firewalls and bypassing security features.

SWIFT Chairman Yawar Shah highlighted the urgency of the situation in remarks at last year's London Business Forum: "The disruptive forces of fraud and cyber have always existed and had to be dealt with in our industry; what is different now is that these threats are more organized, more sophisticated, and more global than ever before."

As part of its efforts, SWIFT published a 16-page report, co-authored by the cyber-security division of BAE Systems, that describes how today's cyber-criminals are infiltrating banks' systems and networks and provides best practices for better securing them.

"The inevitable criminal focus on the heart of the financial system means that the financial services industry needs to ensure it has effective cyber-defenses against well-funded, motivated, and organized attackers," said James Hatch, BAE Systems director of cyber-services.

Cyber-security safeguards

Those in the financial services industry generally acknowledge that stronger safeguards against cyber-threats necessitates industry-wide collaboration, which is the impetus behind SWIFT launching its Customer Security Program (CSP), which aims to improve information-sharing throughout the financial services community and is comprised of its Customer Security Controls Framework.

SWIFT's Customer Security Controls Framework introduces both mandatory and advisory security controls. The deadline for SWIFT users to have implemented and self-attested to the 16 total mandato-

ry controls was Dec. 31, 2017, and they must self-attest at least annually thereafter through SWIFT's KYC Registry.

The SWIFT framework contains 27 controls in total, divided by eight principles, focused on the following three core measures, as summarized in the SWIFT/BAE report:

Secure your environment. Embed security into the design of the bank's network architecture, including physical security measures—such as limiting access rights to authorized personnel as it concerns sensitive areas and ensuring processes are in place to actively control and monitor who is accessing those areas. Additionally, authorized personnel must be properly screened and trained.

Banks should further ensure that they have in place robust and clearly defined perimeter security, with appropriate prevention measures like firewalls and filters, and detection capabilities in case of intrusion. Through the construction of multiple barriers, they should segregate internal networks according to business needs and risk requirements and actively monitor internal networks.

The bank's most critical systems should be isolated from the internet, and a further layer of defenses and detection measures should be deployed. "As a matter of course, you should install the latest versions of anti-virus and system software and immediately implement the latest security updates," the SWIFT/BAE report states.

Know and limit access. After building defenses to prevent hackers coming through the front door, operating procedures and processes must be put in place to then limit and protect administrator and system privileges. This demands the implementation of strong ID management, with strict and actively managed profile and password rules to ensure basic access controls. Additional access controls—such as two-factor authentication across all sensitive or critical applications—should be used to provide another layer of defense.

In addition, banks must identify and protect access rights to all critical systems like interfaces to SWIFT and other payment gateways. "These access rules should clearly allocate rights and capabilities to separate roles and ensure that no single operator can—intentionally or otherwise—open systems to potential abuse," the SWIFT/BAE report states.

Detect and respond. Having in place adequate intrusion-detection capabilities is the third core measure. Banks should actively monitor networks and systems activity, including interfaces to SWIFT, for unusual behavior—such as users logging in at random times of the day or from new or unknown systems, or multiple failed password attempts. Where gaps in capabilities or layers of defense are identified, consider employing the help of cyber-security professionals to ensure the local environment is sanitized and properly defended with the latest anti-virus applications.

> "The disruptive forces of fraud and cyber have always existed and had to be dealt with in our industry; what is different now is that these threats are more organized, more sophisticated, and more global than ever before."
>
> Yawar Shah, Chairman, SWIFT

To be clear, SWIFT is focused on the infrastructure connected to its messaging platform, and thus its Customer Security Controls Framework is "not intended as a be-all and end-all framework for all banks," says Steven Grossman, vice president of strategy at cyber-security software provider Bay Dynamics. "It's all about strengthening the security of all 11,000 banks as they connect to and use the SWIFT messaging platform and making sure they know who is doing those transactions."

"This entails strong authentication, monitoring the behavior of users with tools such as user and entity behavior analytics, making sure there's a segregation of privileges so one person doesn't have too much access and control, implementing proper segmentation between the banks and SWIFT environment, and more," Grossman adds. "It's really about making sure that those parts of the banks that are connected to the SWIFT platform, and the transactions they perform, have the strongest security at all times."

Counterparty risk

Financial institutions must consider not just their internal cyber-security risks, but their interactions and relationships with counterparties as well. Understanding counterparties' credit and compliance risks should be a determining factor in whether and how to do business with them, and cyber-considerations should form an integral part of these routine know-your-counterparty processes, the SWIFT/BAE report states.

As of January 2018, banks that use SWIFT's messaging platform are now able to assess who they are doing business with by requesting their self-attestations against SWIFT's Customer Security Controls Framework to ensure counterparties are taking the necessary precautions and protections.

"Financial institutions in major economies and high-risk jurisdictions are increasingly looking to adopt financial crime compliance tools to show correspondent banks that they have strong controls in place," says Paul Taylor of SWIFT's financial crime compliance division. "This enables them to be a lot more transparent in terms of the controls they have and the lists they are screening against," he says.

That should provide some comfort to correspondent banks that their bank counterparties have security controls in place. "The argument there is if you're a counterparty that doesn't have risk and control solutions in place and a good framework and good diligence around how that works, then you might not necessarily be an attractive counterparty to continue business with," Taylor says.

Findings from a recent anti-money laundering and sanctions compliance survey conducted by AlixPartners speaks to that point. According to that survey, 63 percent of 361 respondents from financial institutions said they've experienced de-risking in their operations in one form or another. Financial institutions have sought to—and continue to—reduce perceived risk by eliminating portfolios, counterparties, or entire lines of business.

For its part, SWIFT has introduced a new module, Correspondent Monitoring, to help banks address money-laundering risk within correspondent banking networks. Correspondent Monitoring allows banks to analyze their SWIFT message traffic to uncover unusual activity patterns and risk exposures within their correspondent banking networks. For example, a user can find out whether it was in receipt of transactions originating in a country considered high risk or subject to sanctions via correspondents operating in a low-risk jurisdiction.

Also related to correspondent banking due diligence, the Wolfsberg Group, a non-governmental association of thirteen global banks, announced significant revisions to its correspondent banking due diligence questionnaire (DDQ) in response to evolving regulatory expectations and industry practice, released in February 2018.

Concurrently, SWIFT announced that it would be aligning its KYC Registry with the new Wolfsberg DDQ for correspondent banks. KYC Registry members can now answer every Wolfsberg DDQ question directly on the KYC Registry platform, increasing transparency and streamlining due diligence processes.

Aside from cyber-security processes and KYC diligence, information-sharing between banks is another vital part of fending off a cyber-attack. Thus, SWIFT is urging banks that are targeted or breached to share all relevant information and alert SWIFT as soon as possible, so that it can share anonymized information on indicators of compromise in the SWIFT environment to limit further damage. ■

Mandatory security controls	Control objective
1. **Restrict Internet Access and Protect Critical Systems from General IT Environment**	
1.1 SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.
1.2 Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator-level operating system accounts.
2. **Reduce Attack Surface and Vulnerabilities**	
2.1 Internal Data Flow Security	Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.
2.2 Security Updates	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.
2.3 System Hardening	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.
3. **Physically Secure the Environment**	
3.1 Physical Security	Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.
4. **Prevent Compromise of Credentials**	
4.1 Password Policy	Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.
4.2 Multi-factor Authentication	Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.
5. **Manage Identities and Segregate Privileges**	
5.1 Logical Access Control	Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.
5.2 Token Management	Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used).
6. **Detect Anomalous Activity to Systems or Transaction Records**	
6.1 Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.
6.2 Software Integrity	Ensure the software integrity of the SWIFT-related applications.
6.3 Database Integrity	Ensure the integrity of the database records for the SWIFT messaging interface.
6.4 Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.
7. **Plan for Incident Response and Information Sharing**	
7.1 Cyber Incident Response Planning	Ensure a consistent and effective approach for the management of cyber incidents.
7.2 Security Training and Awareness	Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.

Source: SWIFT

Collaboration enhances risk management in financial services

The OCC recently endorsed collaboration between banks as a way to reduce costs on managing third-party risk, and compliance officers are more than ready for it. **Jaclyn Jaeger** has more.

Collaboration among financial institutions is how many banks today are enhancing their third-party risk management programs.

Although collaboration is not a new concept among banks, the Office of the Comptroller of the Currency (OCC) recently endorsed it as an acceptable means for banks to alleviate the significant cost burdens associated with a third-party risk management (TPRM) program. That endorsement came in the form of a supplemental guidance (Bulletin 2017-21) the OCC issued in June 2017, which discussed, among other areas, the use of collaboration for managing third-party relationships.

The OCC guidance should come as a welcome development for compliance and risk officers in the financial services industry, as it provides banks substantial flexibility to enhance their own individual third-party risk management programs. "They're really embracing a best-practices approach and one that gives us all more guidance and instruction on what we need to be doing to make sure the regulators are happy," Brad Keller, senior director of third-party strategy at Prevalent, said during a Compliance Week Webinar on the OCC guidance.

OCC Bulletin 2017-21 was issued in response to questions submitted by banks as a follow-up to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance." Issued in 2013, Bulletin 2013-29 provides a comprehensive framework for banks for assessing and managing risks associated with third-party relationships.

In Bulletin 2017-21, in response to questions about collaboration, the OCC responded that when banks use the same service providers to secure or obtain like products or services, they may collaborate to meet certain expectations described in OCC Bulletin 2013-29—such as performing due diligence, contract negotiation, and ongoing monitoring responsibilities. "Collaboration can leverage resources by distributing costs across multiple banks," the OCC stated.

The OCC further stated that banks may take advantage of various tools designed to help them evaluate third-party service provider controls. In general, these types of tools offer standardized approaches to perform due diligence and ongoing monitoring of third-party service providers by having participating third parties complete common security, privacy, and business resiliency control assessment questionnaires. Once third parties complete the questionnaires, the results can be shared with banks.

To gauge how banks are embracing collaboration as outlined in Bulletin 2017-21, Compliance Week conducted an online poll during the Webinar. In that poll, the plurality of respondents (44 percent) said their institution "fully understands the benefits of a more collaborative approach and is investigating how to leverage them in our TPRM program."

The second highest number of respondents (33 percent) said their "institution is unsure how to utilize/execute a collaborative approach in our TPRM program," while 15 percent said their institution is "actively engaged in collaboration with other banks with whom we share common third-party service providers." Nine percent said their institution is "unsure of the actual benefits from a collaborative approach."

Executing collaborative efforts

CCOs and risk officers at banks seeking guidance on how to execute a collaborative approach in their TPRM program may want to check out a policy paper issued by the OCC in 2015. That policy paper described ways that banks currently collaborate, including through the exchange of information and ideas.

Other collaborative efforts used by banks, the OCC said, include:

» Jointly purchasing materials or services;
» Sharing back-office or other services;
» Sharing a specialized staff member or team;
» Jointly owning a service organization;
» Participating in disaster mitigation agreements; and
» Jointly providing/developing products and services.

OCC Bulletin 2017-21 also discussed collaboration opportunities to help mitigate cyber-threats to banks, as well as to their third-party relationships, including engaging with information-sharing organizations. "Banks participating in information-sharing forums have improved their ability to identify attack tactics and successfully mitigate cyber-attacks on their systems," the OCC noted.

The OCC cited a variety of information-sharing organizations that help banks monitor cyber-threats and vulnerabilities and enhance risk management and internal controls. These organizations include the Financial Services Information Sharing and Analysis Center (FS-ISAC), the U.S. Computer Emergency Readiness Team (US-CERT), and InfraGard, among others. Banks also may use the FS-ISAC to share information with other banks, the OCC said.

Bank-specific responsibilities

The OCC has repeatedly warned, however, that collaboration cannot be used to satisfy all oversight responsibilities, particularly third-party risk management processes that must be tailored to each bank's specific needs. Examples of individual bank-specific responsibilities include:

» Integrating the use of product and delivery channels into the bank's strategic planning process and ensuring consistency with the bank's internal controls, corporate governance, business plan, and risk appetite.
» Assessing the quantity of risk posed to the bank through the third-party service provider and the ability of the bank to monitor and control the risk.
» Implementing information technology controls at the bank.
» Ongoing benchmarking of service provider performance against the contract or service-level agreement.
» Evaluating the third party's fee structure to determine if it creates incentives that encourage inappropriate risk taking.
» Monitoring the third party's actions on behalf of the bank for compliance with applicable laws and regulations.
» Monitoring the third party's disaster recovery and business continuity time frames for resuming activities and recovering data for consistency with the bank's disaster recovery and business continuity plans.

Furthermore, the OCC stressed that any collaborative activities among financial institutions must comply with antitrust laws, and that banks should take appropriate steps to ensure compliance with these laws. In this regard, financial institutions should review the Federal Trade Commission and U.S. Department of Justice's joint "Antitrust Guidelines for Collaborations Among Competitors."

Ongoing monitoring

Another focus area for examiners is what banks are doing from an ongoing monitoring standpoint for each of the bank's third-party service providers that support critical activities, which Bulletin 2017-21 also discussed in broad detail.

OCC's 2013 guidance provides specific criteria that a bank's board and management may use to identify its critical activities, but some examples can include

significant bank functions—such as payments, clearing, settlements, and custody—or significant shared services, such as information technology. Other potential critical activities may be those that:

» Could cause the bank to face significant risk if a third party fails to meet expectations;
» Could have significant bank customer impact;
» Require significant investment in resources to implement third-party relationships and manage risks; or that
» Could majorly affect a bank's operations if the bank must find an alternative third party or if the outsourced activities must be brought in-house.

When a bank does not receive all the information it seeks about third-party service providers that support the bank's critical activities, the OCC said it expects the bank's board of directors and management to:

» Develop alternative ways to analyze these critical third-party service providers;
» Establish risk-mitigating controls;
» Be prepared to address interruptions in delivery—multiple payment systems and multiple telecommunications lines in and out of critical sites, for example;
» Ensure that contracts meet the bank's needs; and
» Retain appropriate documentation of all related decisions and efforts to obtain information.

Ongoing monitoring involves looking at not just the bank's third parties' threat environments for areas outside of contractual requirements, but also the threat environment of the sub-contractors. Areas to monitor could include legal activity that could impair the third party's ability to deliver services; regulatory actions; financial viability; operational issues like a merger or acquisition or any senior-leadership changes; or brand and reputational issues.

"Ongoing monitoring lets you address issues before they become events," said Keller, who has been developing and leading risk management programs for more than 25 years. For example, a third-party vendor doesn't have to alert a bank to a data breach that occurred at a data center other than where the bank's sensitive data is stored, but that's something the financial institution ought to know, because both locations likely employ the same IT security controls, he said. Thus, the bank's chief compliance or risk officer should have that conversation with that third-party vendor to determine what they're doing to address that threat.

Another critical piece to ongoing monitoring is documentation. Examiners are going to want to see how the bank's compliance function is executing ongoing monitoring and evaluating third parties' processes against the bank's specifically identified criteria, Keller said.

"No matter how robust the bank's third-party risk management processes are, if those efforts are not documented and compliance cannot provide actual evidence of that process, the OCC, for all intents and purposes, will treat those efforts as non-existent. "It becomes something they view more as aspirational on behalf of the institution, as opposed to something they can say the institution is, in fact, actually doing," Keller said.

A third helpful guidance for compliance and risk professionals in financial services to peruse is OCC Bulletin 2017-07, because it describes what examination procedures OCC examiners may use during the examination of a bank's risk management of third-party relationships. "If you haven't looked at 2017-07, I would suggest you do, particularly if you think you're up for an examination soon," Keller said.

In another polling question provided during the Compliance Week Webinar, respondents were asked to describe their financial institution's response to OCC examination procedures. Most (52 percent) said they treat them the same as any other regulation, while 32 percent said they treat them as an "indication of preparedness."

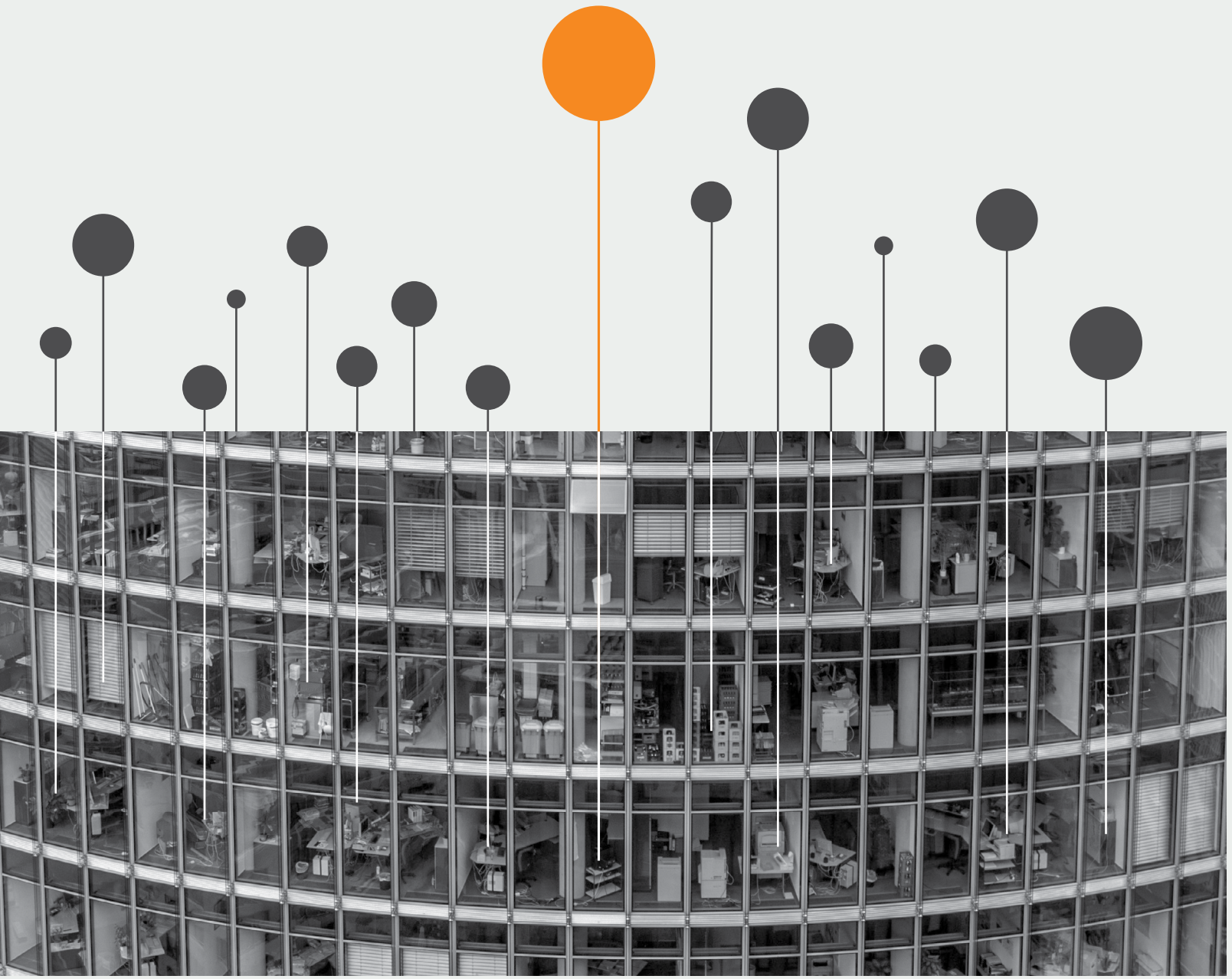
Another 16 percent of respondents said they treat OCC examination procedures as informational, rather than as a regulatory requirement. "The best approach," Keller said, "is to treat it as any other regulation." ■

No one can help you know your customer like Thomson Reuters.

World-Check Risk Intelligence

Trusted around the globe, World-Check powers a range of compliance solutions that enables fast effective remediation to help safeguard organizations from financial and reputational damage.

risk.tr.com/worldcheck



The intelligence, technology and human expertise you need to find trusted answers.

the answer company™
THOMSON REUTERS®