Getting it Down, Soundly:
Dictation and Transcription for Financial Institutions in the Age of Big Data

Dictation and transcription services have been an indispensable business tool for more than a century. From Thomas Edison’s 19th century phonograph, to recordings on wax, to vinyl “memo disks” of the 1940s, to various iterations of the cassette recorder, through to the digital recordings of the 1990s and today’s advanced speech-to-text programs, voice documentation has endured as an efficient means of transferring thoughts, impressions, ideas and inspirations from mind to paper.

Yet dictation technologies have each carried with them challenges. Tinfoil tore, giving way to wax cylinders; cylinders were later abandoned for plastic discs, which were then replaced in the 1950s by magnetic tape. Cassettes of the 1960s and 70s required significant physical storage costs and cumbersome retrieval systems. And today’s best automated voice-to-text programs still can’t replicate the interpretive ability of the human ear.

In an era of tight budgets and shrinking support staff, dictation and transcription services continue to serve a critical role in business. For financial services companies challenged by low interest rates, tighter regulations and shrinking budgets, competitive advantage depends on the timely capture of details of client conversations, business dealings, forecasts and fresh ideas. Yet most managers and even many executives no longer have the luxury of buzzing the secretary in. They’re logging any given workday en route to conferences, at client offices, or in meetings on the other side of the globe. They need documentation solutions that are flexible, accessible and fast.

While dictation and transcription alone are foundational tools, when it comes to data, financial services organizations’ needs are anything but simple. This technical brief has been created in an effort to help financial institutions identify and procure dictation and transcription services that meet their business needs while keeping pace with today’s complex data risk management environment.
This white paper is intended for financial institutions to use as a guide to choosing dictation/transcription services that meet a range of complex legal, compliance and security goals. These needs vary from institution to institution and for that reason this paper is not intended as a single source of guidance on these topics. Rather, this paper is intended to suggest broad issues for awareness and further investigation.

**Big Data, Bigger Oversight**

Given the advanced state of technology today, dictation and transcription are an easy order for a service provider to fill. Thousands of companies — from one-person, home-based shops to multinational organizations with representatives spread across the globe — are standing ready to supply innumerable high and low-tech solutions.

An easy grab for a financial services company? Not so fast. Enter Big Data and a corresponding wave of complex legislation. HIPAA, GLBA, Sarbanes-Oxley, the Dodd-Frank Act and other federal regulations, as well as a tangle of state mandates require financial companies to treat customer data — in particular, personally identifying information (PII), non-public information (NPI), and protected health information (PHI) — with special care. Sanctions for noncompliance can be huge, in some cases in the millions of dollars.

Say a fund manager wants to record the details of a conversation with a client. The information the fund manager discloses to the transcriber may contain a jumble of PII, NPI, trade secrets and other, less sensitive material. In an outsourced situation, that data is now in the hands of a third party. Yet it’s the responsibility of financial institution to keep it safe. “The bank owns the responsibility for due diligence with any supplier,” said one former global risk management executive. A host of regulations governs due diligence requirements, including knowing where the data is held, what protections are in place to safeguard against compromise, and when and how it will be destroyed.

Depending on the type of information held by the service provider, from executive to-do lists to notes following a confidential client meeting to trade secrets, pertinent regulations can include:

- Gramm-Leach-Bliley
- 201 CMR 17
- HIPAA
• PCI DSS
• Sarbanes-Oxley
• SEC rules 17a-3 and 17a-4

Given the complexity of the rules contained in these laws and the consequences of violating them (which include hefty fines), financial services firms must quickly discern whether a service provider can speak the language of compliance. When a prospective client requests documentation of the provider’s media handling policies, for example, the provider should understand not just what to produce, but the rationale behind the inquiry. A risk management culture, in which service provider employees at all levels understand the basics of their clients’ regulatory environment, further ensures the organization will act as a partner in safeguarding against situations that could lead to regulatory violations and other problems.

In considering a service provider, questions should be asked about the basics of risk management policy and accountability, such as:

• Does the company have a defined process for evaluating and handling risks? Is the process adequate for the range of business assets and reviewed annually?
• Does the company have defined policies for protecting the confidentiality, integrity and availability of its information assets? Is the policy based on the ISO 27002 or another internationally recognized standard?
• Is the security policy reviewed annually and communicated to all relevant parties inside the organization?
• Is insurance coverage in full compliance with state and federal laws?

In each case, documentation should be requested. Lack of documentation of compliance protocols should be red flagged for investigation and possible remediation prior to any engagement.

Service providers should understand that different organizations’ risk tolerances result in different formulations for what constitutes adequate and “safe.” While one client may be satisfied with a simple overview of compliance-related policies and procedures, another may require a full-scale audit. Service providers should be open to their clients’ varying needs and tolerances.

Fundamentally, financial institutions that lack a thorough understanding of their own risk profile will be challenged in outsourcing when the relationship involves sensitive data. While larger institutions can rely on in-
house legal teams, compliance experts and robust technologies that identify critical information and discover compliance red flags, smaller organizations often have far less support. A provider that can be relied upon for risk management expertise can prove an invaluable partner.

Vulnerability, Security and Trust

Financial institutions have always succeeded through their ability to win the trust of those who use their services. In ancient Egypt, temple grounds served as the first bank vaults, holding stores of gold safe. Later only European royalty and influential families were seen as sufficiently trustworthy to safeguard the people’s funds. When banks prove themselves vulnerable to risk, the public’s response can be devastating, as when the Texas Republic made banking illegal under the first state constitution following the panic of 1837.

Today, as public anxieties reverberate from the economic crisis of 2008, banks must continue to instill and maintain public trust. Yet the banking environment has never been more complex. Funds change hands via computer; billions of bits of personal information are stored on servers around the globe. Threats have become the stuff of science fiction novels: hacks of corporate networks by rogue states; international identity crime rings; burgeoning data-resale markets; insider heists. Social media, mobile computing and data stored in the cloud further complicate the landscape and add to the variety of criminal entry points. And for banks there is a lot to lose: one breach can irreparably damage an institution with a decades-long history of consumer trust.

Adding to the complexity, financial firms from the smallest community banks to global institutions rely on a host of providers to perform a multitude of noncore, data-intensive functions. Some providers are sophisticated when it comes to security, some less so. While a company has a lot to gain by choosing the best service available, no financial institution can afford to consider a provider that cannot clearly demonstrate its understanding and use of data security protocols.

When a bank is outsourcing services that involve sensitive data, “the first and foremost issue would be around confidential information being protected from unauthorized disclosure or modification, e.g., by using encryption, locked containers, or tamper-evident packaging which reveals any attempt to gain access,” said Mike Dempsey, a former lead examiner with the Federal Reserve who is now with KPMG’s Financial Services Regulatory Advisory – Safety and Soundness practice.
“We would expect the service provider to be fully aware of information security requirements on the protection of firm and client confidentially,” said one vendor management executive at a global financial services firm, when asked about engaging documentation services.

Another top-level concern, said Bob Jones, senior consultant with The Santa Fe Group and contributor to the company’s international standards for service provider assessments, is the security of electronic files. “That’s among the most potentially troublesome areas,” he said. “How susceptible are the company’s servers to a wholesale breach?”

At a minimum, said Dempsey, the service provider should demonstrate it enforces strict protocols for safe and confidential handling of data, including storing all client data on servers protected by 128-bit encryption.

Financial institutions should also ask transcription service providers whether they:

- Run antivirus software with signature files and automatically update them daily
- Use a segmented network with multiple firewalls
- Maintain active intrusion detection systems
- Destroy media that contains confidential data
- Monitor their systems for unusual activity
- Allow wireless device access on any of their networks
- Make appropriate use of encryption to protect sensitive data in transit and at rest

Additional security essentials include:

**Employee background checks.** Are thorough employee background checks conducted, including Social Security number verification and address history, as a requirement for employment? Can transcriptionists access data about the client, or is client data kept separately? Is the dictated information associated with the client’s identity, or does the service ensure a barrier between dictated material and the data’s owner?

**Remote facilities.** Are the equipment and facilities under the provider’s direct control? Is the transcript being processed in the US or overseas? (Only facilities located in the US are required to conform to US laws.) Does the company use home-based transcriptionists?
**Downstream vendors:** Is the workforce processing the work under sole control of the transcription company (or is the vendor hiring “downstream” vendors)?

**Shared environments:** Are the equipment and facilities shared across multiple purposes or companies? Shared environments include a home-based transcriptionist using a personal laptop or a dictation company sharing server space with other companies.

No company can guarantee its systems won’t be compromised. For this reason, financial institutions should ask about incident response plans. A company’s ability to respond quickly and thoroughly to a data compromise, working in partnership with clients, can significantly mitigate financial, reputational and other damage.

Here, regulations come into play in the form of notification requirements. “If an organization discovers a security breach of PHI or PII has occurred, they must respond within very specific timeframes and provide proper notification to affected individuals to protect them from ID theft and fraud,” said Rick Kam, president and co-founder of data breach recovery organization ID Experts. “Besides these federal laws, organizations may fall under state security breach notification laws, which have similar requirements.”

Finally, who in the organization bears ultimate accountability in the event of a security incident? Ideally, the company has a seasoned CISO or other security leader in place on the executive team. Talk with that person about the security environment. What is her view of the complexities of maintaining data confidentiality? Where does she see data security in six months, or ten years? How does her team manage the use of personal technologies? These conversations should yield a good understanding of the company’s position on security and how issues will be addressed.

**What About My iPhone?**

Dictation and transcription services, so long the province of support personnel, are still often viewed as no more than simple, low-level functions. Employees, from multinational CEOs to branch receptionists, are becoming increasingly comfortable “hiring” their own personal technologies — tablets, smart phones, cloud applications — to do their support work. Why not?
The reasons, of course, are myriad. Yet policies to limit these risky practices are falling on deaf ears: according to a 2012 CIO poll, 93% of today’s employees admit to violating company policies designed to prevent information leakage. A key source of risk here is bleed — once a fund manager begins using his iPhone for innocuous to-do lists, might he then, in a pinch, use it for some quick notes on an important client briefing?

Siri and Android’s speech-to-text functions are considered safe, native applications, with data being processed only on the phone. The trouble — in addition to risk of loss of the device itself — is the trustworthiness of the application coupled with complex data use agreements so often dismissed with a touch of the “I accept” button. Rather than holding the content on the device, many speech-to-text applications retain and process the data. Out of the organization’s hands and untraceable, the data may be transferred, copied and even sold, creating serious reputational and compliance risks.

Voice-to-text software can be an attractive option. However, significant barriers to efficiency still exist. These types of software are highly interpretive, and cannot be relied upon for accuracy. Because of these limitations, the time saved through instant voice transcription is more than made up for as the transcriber reads through, corrects and re-reads the transcript. Worse, licenses for voice to text software often require consent to expansive privacy policies — policies that can be prohibitive for a financial institution.

Some questions to ask providers of technology solutions include:

- Is the provider equipped to meet accuracy requirements and can they meet them on day 1?
- Is the service able to handle industry jargon and potential elevated accuracy requirements based on context?
- Does the service have adequate quality control measures in place?
- Does the firm allow customers to direct how transcribed material is delivered (force encryption, limit domains)?
- Is the dictated data only used directly and as needed to deliver transcription?
- Is the firm’s privacy policy compatible based on type of information dictated?
- Does the company have an established and comprehensive data retention policy?
- Is the firm willing and able to participate in an audit to evaluate the security of its systems and facilities?
- Can we afford to spend considerable CPU and memory resources to support the technology?
With personal technologies risky and voice-to-text solutions still lagging, financial services companies must identify better alternatives. A solution must be:

- “Always on” — available 24X7
- Accessible from anywhere
- Easy to use — as easy or better than one’s personal technology
- Able to understand and interpret industry jargon

Cumbersome or slow services, or a lack of documentation services altogether, can lead busy managers to forgo essential record keeping (it’s too hard, I’ll just jot down a few general notes). In a competitive business environment, this can be risky. Critical client details, creative ideas, fresh strategies and urgent to-dos form the foundation of innovation and efficiency on which the best organizations are built.

Worse, if a service fails to meet the bar for ease of use, busy workers juggling multiple projects, deadlines and travel schedules will simply revert to their own equipment (I’ll just store it in my iPhone for now), leaving the information without backup, encryption or other safety measures, creating risks of compliance issues, hefty fines, reputational damage and other problems.

**The Right Provider**

As the pace of business continues to quicken and the scope of individual workers expands, companies will continue to need portable, efficient, always-on technologies to capture fresh ideas and keep critical records.

While documentation remains a simple person-to-person exchange, the surrounding landscape can make selecting the right provider a high-stakes endeavor. Big Data has fundamentally changed the questions financial institutions must ask to mitigate the tremendous risks involved in safeguarding billions of bits of information.

Still, finding a service provider need not be complicated. A few questions can narrow the field considerably. Does the provider have a solid understanding of the risk and regulatory environment in which financial institutions operate? How has the organization’s leadership established a culture of security within the organization? Are employees screened carefully? Are standard protocols for safeguarding data being followed?
Participation in a consortium of security professionals, such as the Shared Assessments Program [link], is another good indicator that the company is committed to risk management and engaged in the larger risk management community.

Finally, while we all enjoy hearing words of assurance in the face of risk, the fact is that risk will exist. All service providers whose work involves touching sensitive data — from dictation to financial modeling to payment processing — should know this. Yes, their job is to support financial institution clients in adhering to rules and preventing compromises. But it doesn't end there. The era of Big Data is only beginning, and risk changes all the time. The right provider acts as a partner, supporting institutions as they navigate this new and highly complex world.