# ARTICLES
# and
# POSTS

# RANTS

Irreverent riffs on
law firm advertising
and other marketing communications

# Creative Corner – The B-Word

by Andy Edelstein on May 18, 2013

Of all the industry categories I've encountered over the last few decades, I've never seen anything quite like the ambivalence with which law firms greet the word "brand."

Reactions to the word range, more or less, from grudging acceptance to outright hostility. One COO of my acquaintance actually bans what he calls "the B-word" at his firm.

What accounts for this?

Well, from a marketing standpoint, law firms are unusual, in that there is a built-in tension between the firm itself and the individual attorneys who work there. When the firm's fortunes rise or fall with those of a few "stars" in their ranks, it's hard to make the case for a firm brand. A star might be considered a brand, but how much of that brand accrues to the firm? And how much remains if that star picks up and leaves?

On the other hand, a strong brand can do many good things. It can be a law firm's protection from the loss of any one attorney or practice group. It can serve as the "tie-breaker" in close pitch situations. It can build a "reservoir of goodwill" in the marketplace — a reservoir from which you can draw in leaner times.

But another reason brands are so important is that your firm surely has one, whether you acknowledge it or not. Your firm's track record, sweet spots, and shortcomings are already out in the marketplace — and they have been for some time. I would collectively call these things a brand, but it doesn't really matter what you call them — they need to be tended to.

Here's the point: If you're not shaping your brand, the marketplace will shape it for you. And you might not like how it comes out.

A brand needs to be built. It needs to be thought through and communicated to the firm's logical prospects. It needs to transcend the reputation of any one attorney or practice group. It needs to represent — and be based on — the firm "as it really is," matching your demonstrable strengths to the needs of your market.

"Brand" is a five-letter word, not four. Your firm needn't think of it as the B-word.


*Andy Edelstein is a copywriter specializing in law firm advertising and marketing communications. Reach him at andrew.edelstein@verizon.net.*

# Creative Corner: Adjective Abuse

by Andy Edelstein on September 18, 2014


Andy Edelstein

Among the many crimes against English routinely perpetrated in the name of legal marketing, there are few, to my mind, more egregious than the wanton overuse of adjectives.

Let me clarify. When I say adjectives, I refer not to the old Anglo-Saxon workhorses we learn in elementary school — *good, bad, hard, easy, fast, slow,* etc. — though even these must be used sparingly and with great care.

Nor do I refer to the deft coloring of a sentence by experienced writers who instinctively understand the limits, and act within them — I am, I admit, fond of my own use of "egregious" and "wanton" in the first sentence of this piece.

No, my quarrel is with those vague generalities that seem to squeeze the air out of most legal marketing communications. The same offenders appear over and over: *preeminent, collaborative, responsive, client-focused, business-oriented, collegial, innovative, entrepreneurial, strategic, authoritative*. The list goes on. You could probably add a few yourself.

While the qualities described by these words are, perhaps, desirable traits in a law firm, the words themselves are empty, bordering on meaningless. They beg to be replaced with specific explanations.

If your firm is truly *innovative*, why not tell us something new? If you want to be seen as *collaborative*, wouldn't an exploration of client teams — at minimum — be in order? If you pride yourself on being *client-focused*, how are you different from the gazillion other firms saying exactly the same thing? And if you claim to be the *preeminent* firm at anything, why on earth should we take your word for it?

My point is that the adjectives alone won't do. At best, they make the firm sound dull. Whenever you see one — especially from the list above, especially from your own firm — proceed with caution.

Adjective abuse may only be a misdemeanor, but it's a serious one. Your creative license could be suspended.


*Andy Edelstein is a copywriter specializing in law firm advertising and marketing communications. Reach him at andrew.edelstein@verizon.net.*



Previous post: Creative Corner: Law Firm Marketing?? Questions Can Resolve the Questions

# Creative Corner: Table Stakes

by Andy Edelstein on November 23, 2014

In poker, *table stakes* are the chips a player must ante up to get in the game.

In marketing, the term has come to mean the minimum offering a product must have to go on the market. It refers to the features a consumer expects, insists on, and assumes will be included in the product.

You can't, for example, put a new smartphone on the market without certain essentials — a camera, a keypad, a standard operating system that accepts apps, etc. To not have these things is unthinkable. The consumer expects them, so they'd better be there. Without them, your product will fail.

Good marketers never waste time, space, or scarce marketing dollars talking about table stakes. Yet in law firm marketing communications, you see table stakes mentioned all the time, usually in the form of abstract generalities that should literally go without saying.

How many times have you seen the phrase "*focused on our clients*" on a law firm website — perhaps even your own? Does this phrase differentiate the firm in any way? Does it convey, in itself, any proof of the firm's client focus?

Not that client focus is a bad thing — if I were your client, I would certainly want you to focus on me. But if I were shopping for a law firm, I'd expect nothing less from every firm I talk to. So even if you have great client focus — even if the ways you focus on your clients are truly differentiating — you'll need to work harder to prove it to me. The phrase itself will never convince me. It's table stakes. It's like advertising a car by saying it comes with a steering wheel.

Table stakes are, regrettably, omnipresent in legal marketing. Words like *quality*, *collaboration*, and *excellence* appear everywhere, but their meanings are entirely in the eye of the beholder. They are generalities — if you can't successfully demonstrate or prove them, why even mention them?

One particular table stakes word stands out, not just for its irrelevance, but also for its ability to backfire on the firm that uses it: *integrity*. As soon as you use it, you lose it. Lawyer jokes aside, most prospects assume your firm has integrity — unless something calls it into question. Mentioning it does just that. It makes the reader wonder why you're calling attention to something that should certainly be considered table stakes.

# Creative Corner: What advertising can — and can't — do

by Andy Edelstein on October 20, 2012

 As budget season approaches for what many predict will be at best a so-so year in Lawland, I humbly ask that you consider — possibly for the first time in your firm's history — advertising.

I plan to spend the next few of my quarterly rants discussing various aspects of this subject, but let me start by saying this will not be an easy sell to your management. Lawyers traditionally have enjoyed a hate-hate relationship with advertising. They hate the very notion of hawking their wares as if they were a tube of toothpaste or a light beer. And they hate the idea of budgeting for what they perceive to be an expensive and ultimately wasteful proposition.

Still, economic pressures would seem to be urging them to get over this. Other professional services categories — brokers, accountants, real estate, etc. — have long since accepted advertising as a valid, even necessary, part of the integrated marketing mix. So have plenty of law firms, whose ads now regularly populate the pages of both horizontal publications (targeting mostly GCs) and vertical trade magazines (targeting industry sectors).

But first, let me clear up a few things about what you're getting into.

**What advertising can do for your firm:**

- Build awareness over time — Some advertising proponents think it's enough just to get your name out there. It's not. But carefully crafted messages about what your firm stands for can gain important traction in the marketplace. It won't happen overnight, but if you do it right, it will happen.
- Amplify your reputation — Note the word "amplify." Your reputation is already out there. Ads will not create it — only your work can do that — but they can create a multiplier effect in terms of how — and by whom — you're perceived.
- Put you into the consideration set — Once potential clients are aware of your existence and reputation — never a given, as you know — advertising can put you in the mind of a potential client when an actual hiring event occurs. This alone will probably not get you the job — but it might get you into the pitch.
- Work with other marketing communications — These days, there are so many ways to communicate to your audience — both online and off — that actual ads have come to serve a dual purpose. First, they deliver messages in their own right. Second, they drive your audience to other places — i.e. your website — where other information can be found. Especially effective is to drive that audience, not to your home page, but rather to a minisite set up specifically to elaborate on the advertising. This idea could take up a whole article in itself, but not now.

- Accentuate the positive — As Don Draper says in one of the first MadMen episodes, "Advertising is happiness." Ads are what you use to put your best face forward, to give people the good news about your firm. They are relentlessly positive, and, when used properly, they can help you build a "reservoir of good will" in the marketplace — a reservoir you may someday need to tap when the news is not so good.
    - Rally your troops — Never underestimate the prestige and pride that accrues to your people when they can say "Did you see our ad?" Think of it as an instant elevator pitch they can point to at any time. If advertising does nothing else, this sort of "cocktail party cachet" is almost worth the cost.

**What advertising cannot do:**

- Make the sale — No client will ever look at an ad and say "Hire that firm." The sales process is far too long and involved for that. But your ads can get you to the point where you can do the other things that ultimately lead to a hiring situation.
- Provide instant gratification — The buildup of advertising awareness is a slow process. You need to be in front of prospects often if you want to make an impression. If you're not willing to put an entire year into an advertising program, don't bother. A single ad in a single publication will do nothing for you.
- Come cheap — Even when advertising is cheap, it's not very cheap. You'll need to spend for creative (writing and design), production (readying it to run), and media (the place where you run it). Corners can be cut, but there's usually a price to pay when you do — a non-monetary price that might come in the form of fuzzy messaging, ugly design, ineffective media, or all three. In the long run, saving money usually ends up wasting it. You should be prepared to spend at least $100K over a year — $300K is even better.
- Show a clear ROI — This has frustrated the biggest advertisers in the world for as long as ads have existed. But you simply cannot put a pile of dollars into one end of the pipe and know there will be a bigger pile emerging at the other end. It doesn't work that way. It's a slow buildup and there are no guarantees it will work. But what those same frustrated big guys all have in common is their total confidence that advertising did — and will continue to — successfully build their brands.
- Replace PR (or other marketing communications) — Advertising always works best when it's part of an integrated marketing effort. For law firms especially, PR will always be at least as important as advertising, and ads can never get out the sorts of granular, in-the-trenches information that good PR provides on a regular basis.
- Overcome bad work — Bad news will always travel faster than good news, and if you have perception problem with your work product, your people, or your reputation, advertising will probably not help you — and it could make things worse. That said, advertising can help you recover from the problem. When it's part of a coordinated crisis management initiative, it can definitely accelerate your comeback.

Advertising is not for everyone. If you can't commit to a real program — designed and executed by real advertising professionals — you are probably better off not doing it.

But it's important to realize that law firms have been painfully slow to grasp what other industries already know: there is simply no better way to raise your visibility among the prospects you want to attract.

*Andy Edelstein is a copywriter specializing in law firm advertising and marketing communications. Reach him at* ***andrew.edelstein@verizon.net***.

Previous post: Fall 2012 Events

Next post: "Crisis Management: Lessons Learned from the Army" – September 20th Evening Program

- LEGAL MARKETING ASSOCIATION LMA METROPOLITAN NEW YORK CHAPTER

- **latest news**

# Creative Corner: Copy v. “Content”

by Andy Edelstein on December 30, 2013

 This may be hard to believe, but before there was an Internet, there was no such thing as “content.” Not the way we mean it now.

Back then, the text that formed the basis of an article or an ad or any sort of marketing piece was called “copy.” It was written by people called “copywriters.” As a long-standing member of that semi-honorable profession, I now find myself bristling at what I feel is the relegation of copy in favor of this upstart term, content.

I know, it’s just a word. I’m probably overreacting. I should get over it.

But please consider: Words carry power — it’s one of the reasons I do what I do. And the power that the word “content” has garnered for itself in recent years undermines, to a significant extent, what I — and my fellow copywriters — do.

To us, content has come to mean something like “the text placed into a web page (or other material) as a required complement to the design.” Often enough, a certain reluctance is implied. When people (almost always non-writers) use the word, it’s often with an undertone of distaste, as if this copy is a necessary evil that serves only to interrupt the elegance of the design.

Words, in other words, have become the supporting cast. Design is the star.

Needless to say, I take issue. We are, after all, working for law firms. What we’re selling is legal work. If we were selling Gucci or Maserati or Calvin Klein, I would happily concede that design should be driving the bus.

But when we sell “Esoteric Securitization” or “Chapter 11 Debtor Representation” or “Employee Benefits Litigation,” where is the dazzling imagery? Where is the elegant visual? Designers, I assure you, do not approach these subjects with enthusiasm. So why should the words have to ride in the back?

Lawyers are word people. Words are their tool, their product, and often enough, their weapon. The same can be said of their main customers: general counsel. To relegate the words to mere content is to say “Yes, we know ‘securities litigation’ is boring, but our marketing people think we need this verbiage on our website, so please feel free to ignore it while admiring our deft use of bold colors to showcase stock photography of gavels and doric columns and courthouse steps.”

The fallacy here is that, as marketers, it is absolutely wrong to concede that securities litigation is boring. To the target audience — actual consumers of securities litigation — it is anything but. If the copy, therefore, is not

compelling, persuasive, and provocative, then new copy is clearly called for. Copy, not content.

As I've said before in these pages, law firm marketers don't pay nearly as much attention to writing as they do to design. As such, they do themselves and their firms a disservice. Admittedly, the rise of the word "content" is a symptom, not the disease. But sometimes addressing the symptom can be a big step toward curing the disease.

*Andy Edelstein is a copywriter specializing in law firm advertising and marketing communications. Reach him at andrew.edelstein@verizon.net.*

Previous post: Journalists' Journal: Monica Bay (Law Technology News) with Tom Mariam

Next post: Sell It, Tell It, Retell It

# Creative Corner: Journalism v. Copywriting

by Andy Edelstein on April 9, 2012

 Having spent much of my career on Madison Avenue, it always gives me pause when a law firm hires a journalist to write a marketing piece.

Nothing against journalists, mind you. I am a dedicated fan of the press in all its forms, and I admire and applaud the standards good journalists strive to uphold. It's just that when it comes to marketing, other standards apply.

As the competition for legal services grows increasingly intense, every piece of communication that comes out of your marketing department is—overtly or covertly—charged with selling your firm.

That's not what journalism does. Journalists are objective—objectivity is their creed, it's what makes them so important to society. Their job is to be impartial, to report a story from all sides, to refrain from bias.

But objectivity is not what marketing is about. Copywriters are trained to tell only the good news. Their job is to show your firm in its best light, blemish-free. They have no obligation to show anything but your good side.

In other words, copywriters don't report, they promote. And while they're certainly capable of great subtlety in the ways they promote, no audience they target is under any illusion about motives.

Yes, there are times when the line between the two disciplines is thin. When, for example, you hold a thought leadership panel and want it written up, there is a temptation to treat the envisioned piece as journalism.

But think about it. If your firm's name is going on the piece, it is, by definition, marketing—not journalism. Even if you adhere to the strictest journalistic standards, you will not be seen as objective. It will be assumed you have an agenda. So why try to dress it up as journalism, when it's not?


*Andy Edelstein is a copywriter specializing in law firm advertising and marketing communications. He can be reached at andrew.edelstein@verizon.net*



Previous post: Journalists' Journal: A talk with Eric Effron, Editor, Reuters Legal

Next post: NYLMA Spring 2012 Chapter Events

# K2 INTELLIGENCE

Posts about corporate investigations, compliance, and cybersecurity

November 19, 2015

# The Threat From Within

**A rogue employee can do at least as much damage as a rogue nation.**

Even as organizations hunker down for a long and expensive siege against attackers from cyberspace, a determined employee with the right kind of access can be as much of a threat, if not more. Whether disgruntled or dishonest, whether destroying records or stealing intellectual property, it is shockingly easy for insiders to wreak havoc on your most valuable digital assets.

Unprotected data can leave your office on a thumb drive, a laptop, or through a personal email account. Once outside, there are plenty of lively markets for it, both online and off. From competitors looking for trade secrets, to criminals stealing customer data, to rogue states breaching national security — and much more — there is no shortage of buyers for any information that can be monetized.

**Are you prepared?**

Far too many organizations are unprepared for insider threats. Their data isn't properly segmented. Password policies are too lax. Mobile devices are insecure. Access permissions are haphazard and not adequately policed.

As a result, a company's crown jewels can be left exposed. Even your most loyal employees — those with no mischief on their minds — will seek out unprotected data simply because it's there and they can access it. The problem escalates when an employee with personal issues — debts, drug use, family issues, etc. — succumbs to the temptation to turn access into opportunity. And when that employee works in IT, or even runs the IT department, the damage can be catastrophic.

In the face of these threats, data security needs to be taken far more seriously than it too often is. The crown jewels must be walled off, with access strictly limited on a need-to-know basis. Checks and balances must be established — IT, compliance, and cybersecurity must be responsible for watching over each other. Policies for activating and de-activating accounts must be tightened.

Most organizations have neither the resources nor the personnel to assess current practices, recommend the proper changes, and institute the stricter policies and procedures necessary to protect data going forward. Professional help is usually required.

**Are your employees trained?**

There is no substitute for instilling the basics of data security throughout the organization. Employees need to be trained by experts in the dos and don'ts. They need to know how to create a proper password. They need to know not to share passwords with co-workers. They need to understand the consequences of insider leaks, even if unintentional.

Email, in particular, is a security breach waiting to happen. Email attachments must not be forwarded to personal accounts. Co-mingling of accounts — work and personal on the same device — need to be restricted, if not eliminated. Awareness of spear-phishing and other "social engineering" ploys needs to be taught and constantly reinforced.

**Do you know how to investigate?**

If you suspect an insider has been tampering with your data, intense scrutiny — of computer logs, of email traffic, of work processes and procedures — is absolutely essential. The goal is to identify patterns of employee behavior to determine where the breach came from, what damage has been done, and who is responsible.

There are many questions to consider: Who recently accessed a particular shared folder — and why? Who is accessing documents they should not normally be seeing? Is someone from finance

Webinars & Events
In the News
Newsroom
Publications
K2 Blog
National Cybersecurity Awareness Month

copying a strategy statement? Is someone from marketing looking at technical specs? Is someone who has always left the office at 5 pm suddenly staying until 8 pm every night?

Once these questions are answered, there is still a great deal of detective work to do: interviewing personnel, narrowing down suspects, examining motives, figuring out how the breach was carried out. For each step in this process, it is best to engage expert help. Your organization is unlikely to possess the skills to either identify the breach or pin down the suspect.

### Are you getting the right help?

It cannot be overstated that for any insider incident, the adequacy of the response will be commensurate with the level of advanced preparation. Policies need to be established, procedures tightened, employees thoroughly trained, and remediation plans carefully laid out ahead of time.

Doing these things right may require outside assistance, but once they're in place, your organization will be in a much better position to prevent breaches in the first place — and to respond to them when they occur.

August 25, 2015

# Tearing Down the Silos

**When AML compliance and cybersecurity work together, both are more effective**

It is no secret that financial institutions have become fat targets for cyber criminals. Stories of spectacular data breaches — of hacking, identity theft, and all manner of suspicious financial transactions — are now as common as they are disconcerting.

Many of these stories involve some form of data intrusion, closely linked to some form of money-laundering. To a bank, these two types of crime have traditionally been two separate concerns, each with its own silo. Data intrusions have fallen under cybersecurity, money-laundering under AML compliance. Communication between the two silos has generally been minimal.

If financial institutions are to effectively combat these threats, it is clear that the silos need to be torn down. Going forward, every suspicious customer activity should be assumed to involve a data breach, while every data breach should be assumed to be a financial crime in the making.

Cybersecurity and AML, in other words, need to work together. Each group can dramatically enhance the effectiveness of the other, and there is simply too much at stake for them to continue working in isolation.

**Different cultures, different mindsets**

The gaps in communication between the two groups are hardly surprising. Each has its own personnel and culture. AML is a compliance function, a natural outgrowth of proliferating financial regulation. Cybersecurity is a technology function, a confluence of IT and security interests. The languages, work processes, and mindsets are fundamentally different.

But despite this, both teams now have much to say to each other. As most of the world's financial information now moves through cyberspace, most financial crime now occurs — at least in part — online.

Where compliance professionals once concerned themselves with check kiting and other quaintly low-tech scams, today's super-sophisticated global frauds move money in and out of multiple IT systems, literally, at the speed of light. It takes a technology mindset — specifically, cybersecurity expertise — to keep up.

At the same time, cyber crime frequently goes hand-in-hand with suspicious financial transactions. Bank accounts, credit card accounts, and ATMs are illegally accessed via "spear-phishing" emails or other "social engineering" ploys. Often, it takes an anti-money laundering mindset to detect the crime — or even to understand that a crime has been committed.

**Two sides of the same coin**

With the bad guys now moving at the speed of light, now the banks must do so as well. What is needed is a freer, more streamlined sharing of information between AML and cyber.

There are plenty of opportunities for cross-pollination. The two groups are both now invested in similar big-data technologies — powerful analytical tools that are used by the cyber team to investigate data breaches and by the AML team to scrutinize suspicious transactions. Integrating these into a single fraud information exchange would go a long way toward making sure one hand always knows what the other is doing.

**Watching the bad guys monetize**

Transaction monitoring is a great place to start this integration. A typical assault on a bank starts with online customer data being stolen. But that data — account numbers, PIN numbers, social

Webinars & Events

In the News

Newsroom

Publications

K2 Blog

National Cybersecurity Awareness Month

security numbers, debit and credit card numbers — has no value to the thieves until they can convert it into cash. This is classic money-laundering, now playing out online.

The AML team — having set up the rules and triggers that detect fraudulent transactions — can provide the cyber team with vital information about dates, times, dollar amounts, and the frequency of all sorts of anomalous activity. The two groups can then work together to cross-reference this information with any spikes in wire transfers, online purchases, ATM withdrawals, or other vulnerable banking activities. In this way, information flowing from AML to cyber can help detect — and prevent — attempts to monetize stolen data.

### Sounding the alarm

Of course, the information needs to go in the other direction as well. Whenever the cyber team detects a breach in the bank's firewall, the AML team needs to hear the alarm. The sooner they know about the intrusion, the sooner they can raise alert levels and heighten scrutiny of suspicious transactions.

Both teams can then walk back the incident to identify any early indicators. What happened in the preceding days, weeks, or even months? Was money moved into or out of suspect accounts? Are there patterns to the suspicious behaviors? While AML works the transaction information, cyber can track the IP addresses involved in the incident. Working together, the two groups can accomplish what neither could by itself.

### A meeting of the mindsets

Successfully bringing the two cultures together is not automatically given, and may require the help of a third party. An astute consultancy — one thoroughly steeped in both cultures — can add value by bridging the gaps in communication and technology, while providing the big-picture perspective gained from working with a wide range of financial institutions.

However, the task is clear. With or without help, AML and cybersecurity must discover what they have in common, identify mutual strengths and weaknesses, and move toward an effective fusion of functions, processes, and mindsets.

July 28, 2015

# The Case for a Proactive Look-Back

**A review of past transactions isn't just good compliance — it's good business.**

All too often, a look-back at a bank's past transactions comes as a reaction, either to a deficiency in its transaction monitoring system or, worse, to an enforcement action.

A look-back might follow years of lax compliance and repeated warnings. It might be triggered by evidence of suspicious transactions. It might even be the result of an intentional but short-sighted business decision to postpone – or even forego – compliance costs.

Whatever the reason, this type of reactive look-back is inherently negative. It is often the gateway to a wider investigation, an onerous enforcement action, and costly remediation. The collateral damage to reputation alone can be severe.

On the other hand, a proactive look-back — one undertaken on your own initiative — can be uniformly positive. At minimum, it can serve to get your compliance house in order. But beyond that, a thorough and conscientious review of past transactions— conducted by an experienced and independent third party — can yield important benefits for your entire organization.

Think of such a look-back as an opportunity to:

### Show diligence

Regulators do not expect perfection — they understand that money laundering will never be completely preventable. However, they do look favorably on compliance programs that are well designed and diligently executed. In their eyes, a proactive look-back can demonstrate a level of rigor that might serve to immunize you against the consequences — legal, financial, and reputational — of any money-laundering activity you may uncover.

### Normalize your data

The gathering of transaction records from multiple sources within the organization can expose a range of data compatibility issues, especially in banks living with the patchwork of legacy systems from past mergers. A look-back requires data from all sources to be placed in a single normalized form — only then can it be analyzed by a transaction review tool. This normalization in itself brings value, reconciling diverse data formats, often for the first time.

### Sharpen your procedures

A look-back can show you the gaps in your AML policies and procedures, especially in the crucial area of know-your-customer (KYC) compliance. If your account opening process is lacking — if the rules are not well conceived, if the red flag thresholds are too low or too high, if the level of scrutiny is not commensurate with the perceived risks — a look-back can show you the weak spots and point you to solutions. Far better to have any deficiencies discovered by you, rather than by regulators — and any remedial actions you take will surely serve you well at your next audit.

### Better understand your risks

The risk profiles from one banking department to another can be substantially different. For instance, a regulator will likely expect a private banking customer to receive more scrutiny than a checking account customer. A look-back can help you focus on relative risk levels, assigning transaction monitoring rules to each department and allocating resources accordingly.

### Uncover suspicious activity

A look-back should lead to improvements in your ability to generate suspicious activity reports (SARs). Any proactive production of evidence — of money laundering, terrorism financing,

Webinars & Events
In the News
Newsroom
Publications
K2 Blog

sanctions violations, or other wrongdoing — will highlight your commitment to vigilance, thus building your credibility with enforcement agencies.

### Detect data breaches

While cyber security is generally considered a separate concern from AML compliance, a look-back at past transactions can reveal data intrusions that may not have been previously detected. The need for information exchange between your AML team and your cybersecurity program cannot be overstated.

### Think strategically

Even as it shines a spotlight on your compliance issues, a look-back can reveal other business issues as well. An analysis of past transactions will often produce actionable insights that can lead to subsequent improvements in data systems, information workflow, and overall operations.

In other words, a look-back is not just about how you appear to regulators. It's about looking at AML compliance strategically, about fitting it comfortably into your overall business objectives. Ultimately, it's about treating your compliance issues, not as a burden to be borne, but as an opportunity to be seized.

New York
845 Third Avenue
New York, NY 10022
+1.212.694.7000

Thacher Associates
A Subsidiary of K2 Intelligence
845 Third Avenue
New York, NY 10022
+1.212.845.7500

London
Albemarle House
1 Albemarle Street
London W1S 4HA
+44.207.016.4250

Madrid
Calle Almagro 15, 5ª
28010 Madrid, Spain
+34.917.021.364

Tel Aviv
89 Medinat
Hayehudim Street
Tower E
Herzliya Pituah
Israel 4676672
+972.9832.6126