

CRIME/FINANCIAL INSTITUTION BOND COVERAGE

What Asset Managers and Broker-Dealers Need to Know

Insights from a Financial Institution Bond Product Manager

Tracey Santor, Travelers Bond & Specialty Insurance



Introduction

Asset managers and broker-dealers hold something every financial criminal wants: direct access to client money. That combination of trust, access, and speed makes registered investment advisors and broker-dealers a persistent target for fraudsters — not because these firms are careless, but because the math favors the attacker. It only takes one successful attempt out of thousands to pay off.

At Liftman Insurance, we have specialized in protecting financial professionals since 1957. Crime insurance — the umbrella that includes fidelity bond coverage (employee dishonesty) along with forgery, computer fraud, funds transfer fraud, and fraudulent instructions — has been part of that work from the beginning.

Recently, we sat down with Tracey Santor, Product Manager for Financial Institution bonds for Travelers, along with Mark Liftman and Angela Dennis of Liftman Insurance, to talk through how employee dishonesty schemes unfold, how fraudulent instructions and social engineering losses happen, where check fraud is trending, and what separates firms that catch these losses early from firms that don't.

This white paper draws on that conversation — real claim scenarios, coverage distinctions that matter, and the practical steps that make the biggest difference — to help you understand your exposure and make informed decisions about your Crime and Fidelity Bond coverages.



Tracey Santor
*Product Manager
for Financial
Institution bonds*

Travelers Bond
& Specialty
Insurance



Mark Liftman
President
Liftman Insurance



Angela Dennis
*Bond Manager/
In-House Underwriter*

Liftman Insurance

What Is Crime Insurance?

Crime insurance is the umbrella term for a family of coverages that help protect financial institutions against theft, fraud, and employee dishonesty along with numerous other coverage grants. Fidelity bond coverage, also known as employee dishonesty coverage, is one piece of that umbrella. It responds specifically to crimes committed by your own employees.

The rest of the umbrella responds to crimes committed by people outside your organization. Forgery, computer fraud, funds transfer fraud, and fraudulent instructions coverage each addresses a different way an outsider can get at your firm's money or your clients' money. None of these coverages overlap with one another — each is its own insuring agreement, and a firm elects which ones to carry.

CRIME INSURANCE AT A GLANCE:

- **FIDELITY** — crimes committed by your own employees.
- **FORGERY** — forged, altered, or counterfeit checks and instruments.
- **COMPUTER FRAUD** — unauthorized computer access used to cause a transfer of money or securities.
- **SOCIAL ENGINEERING FRAUD** — fraudulent instructions that trick a bank into moving the insured's own money.
- **FRAUDULENT INSTRUCTIONS** — impersonation of a customer that causes the customer's money to move.

Table of Contents

CHAPTER 1

Asset Managers and Broker-Dealers Are Prime Targets for Fraud_____ **5**

CHAPTER 2

The Trusted Employee Problem_____ **7**

CHAPTER 3

Fraudulent Instructions and the Power of the Callback _____ **9**

CHAPTER 4

Cyber Liability and Crime Insurance Coverage Aren't the Same Thing_____ **11**

CHAPTER 5

Check Fraud Hasn't Gone Away — It's Gotten Smarter _____ **14**

CHAPTER 6

Real Estate Transactions Are a Favorite Target _____ **17**

CHAPTER 7

Not Every Firm Carries the Same Coverage — and That's a Risk_____ **19**

CHAPTER 8

Five Things Every Firm Should Do Right Now _____ **21**

CHAPTER 1

Asset Managers and Broker-Dealers Are Prime Targets for Fraud

“Financial institutions of every kind are targeted for the same reason. They have access to money, and fraudsters know it.”



The pattern Tracey Santor sees across Travelers' national claims is consistent: financial institutions of every kind — banks, insurance companies, asset managers, and broker-dealers — are targeted for the same reason. They have access to money, and fraudsters know it.

That access makes advisory firms and broker-dealers attractive targets regardless of size. Fraudsters share information about vulnerabilities and tactics on the dark web, and they operate at scale — sending out large numbers of attempts because it only takes one to succeed. A firm doesn't

need to be a household name to be a target. It only needs to hold client money.

“The asset managers and broker-dealers have access to money, and the fraudsters know that. The fraudsters use the dark web to share their information on how to get to that money, so asset managers and broker dealers are targets for the bad guys.” - Tracey Santor

One notable shift Santor has observed since the pandemic: classic employee dishonesty claims — an employee simply stealing from the firm — have declined, while computer-related fraud claims have risen. The threat hasn't gone away;

it has moved from the back office to the inbox.

Santor routinely reviews financial institution bond claims from across the country specifically to identify new scam trends.

BEST PRACTICE: Don't assume your firm is too small to be a target. Fraudsters target volume, not prestige — any firm with access to client funds is a potential mark. Treat fraud prevention as a standing priority, not a response to a specific threat.

CHAPTER 2

The Trusted Employee Problem

With employee dishonesty claims, oftentimes it seems that it's a very trusted employee. They take advantage of that trust to do things that maybe other people would be questioned about. Because they're trusted — they're not questioned.



When people picture employee dishonesty, they often picture an obvious insider or a disgruntled employee. The claims Santor reviews tell a different story: the most damaging losses often involve a trusted, long-tenured employee who used that trust as cover.

"With employee dishonesty claims, oftentimes it seems that it's a very trusted employee. They take advantage of that trust to do things that maybe other people would be questioned about. Because they're trusted — they're not questioned." - Tracey Santor

One example Santor noted: an office manager at a small advisory firm handled the firm's bank accounts, paid invoices, balanced the checkbooks, and managed vendor billing. There was no joint control — no second set of eyes on what she did. She also handled payroll and insurance. After she resigned, the firm discovered she had been stealing money the entire time. That pattern — theft that continues undetected until the employee leaves — is common. In the past, an employee's absence (illness, vacation) often surfaced irregularities when the work crossed someone else's desk. With around-the-clock

computer access, that natural oversight has largely disappeared.

A second example: a head of facilities ran an invoicing scheme with vendors, soliciting inflated invoices in exchange for kickbacks — a traditional fidelity claim that has existed for as long as businesses have had vendors, and one that computer-based oversight hasn't fully eliminated.

On the broker-dealer side, the exposure looks different. The majority of employee dishonesty claims Santor sees involve registered representatives — sometimes selling unauthorized or fraudulent investment vehicles, occasionally amounting to Ponzi schemes — operating without adequate supervision. In several cases, a rep with 15 years of tenure at a firm had been selling bad investments the entire time, undetected.

BEST PRACTICE: Build in separation of duties wherever possible — no single employee should control bank accounts, invoicing, payroll, and client billing without oversight. For small firms that can't fully separate duties, assign someone above that function to periodically review bank activity, invoices, and vendor lists for anomalies.

For broker-dealers: maintain active supervision of registered representatives' outside activity and product recommendations. A long tenure is not, by itself, evidence of trustworthy conduct.

CHAPTER 3

Fraudulent Instructions and the Power of the Callback

Alongside employee dishonesty, Santor pointed to a second major trend that has grown steadily over roughly the last decade: when a customer's money is moved out of an account because of a fraudulent instruction.

Most often, that means someone impersonates a legitimate customer to convince the firm to send money out of the account; it can also mean an insider is deceived into instructing the bank directly.

The mechanics vary. A fraudster may hack into a victim's email account and send withdrawal instructions that appear to come directly from the customer's own address — making the request look completely legitimate on its face.



“ The firm should do a callback to a predetermined phone number to verify that that instruction is real. ”

"They may send an email from an email account that is similar to the victim's... or hack into their computer and actually send emails that are from that person's computer... The best thing to prevent that from happening is the firm should do a callback to a predetermined phone number to verify that that instruction is real."
— Tracey Santor

The single most effective defense, in Santor's assessment, is a callback to a phone number the firm already has on file — never a number provided in the email or message itself. Done consistently, this stops the majority of these attempts.

No verification method is foolproof. Fraudsters have been known to execute SIM swaps — convincing a mobile carrier to transfer a victim's phone number to a new device — which can defeat a callback if the fraudster ends up receiving the call. These cases are rare but not impossible. Voice recognition as a verification method is becoming less reliable as deepfake technology improves, and Santor specifically cautioned against relying on it. An emerging technology called FIDO2 — a cryptographic key that authenticates identity through encrypted

messages rather than a phone call — may eventually offer a stronger alternative, though adoption is still limited.

Firms were once reluctant to adopt callback verification out of concern that customers would find it intrusive. That resistance has largely faded. As Santor noted, customers now tend to appreciate knowing their accounts are being watched over closely.

BEST PRACTICE:

Require a callback to a predetermined, previously verified phone number for every request to transfer money or change account instructions — no exceptions, regardless of how routine the request seems.

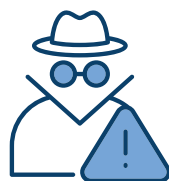
Never call a number provided within the request itself. Use only numbers already on file.

Do not rely on voice recognition alone as a verification method. Watch for emerging authentication technology like FIDO2 as it becomes more widely available.

CHAPTER 4

Cyber Liability and Crime Insurance Coverage Aren't the Same Thing

“ Social engineering in our world means it's our insured's money and not their customer's money. Their customer's money is covered under fraudulent instructions. ”



Firms often assume crime insurance and cyber liability insurance protect against the same losses. Although they may share some insuring agreements such as social engineering or funds transfer fraud, the policies are very different – and understanding the difference is important to prevent gaps in exposures.

The core distinction is what triggers payment. Crime insurance addresses tangible loss: money that is actually gone. It only responds once you can prove the loss occurred – that proof is a condition of the claim. Cyber liability insurance, by contrast, responds to cost and exposure: the expense of hiring forensic investigators, notifying affected clients, responding to regulators, and defending or settling a lawsuit if your firm is sued after a breach. Cyber liability can respond even when no money has actually been stolen – the trigger is liability exposure, not loss of funds.

CRIME INSURANCE vs. CYBER LIABILITY INSURANCE:

- **CRIME INSURANCE** — addresses the actual money lost; you must prove the loss to collect. Covers fidelity, forgery, computer fraud, fraudulent instructions, and multiple other risks.
- **CYBER LIABILITY INSURANCE** — addresses the cost and liability of a breach: forensic investigation, client notification, regulatory response, and legal defense. Responds even without a dollar loss.

One nuance worth knowing: many cyber liability policies bundle in a small amount of crime coverage — often in the range of \$100,000 to \$150,000 — with its own deductible, sometimes \$25,000 to \$50,000. Confirming your actual crime insurance limits on a dedicated policy, rather than relying on what's bundled into a cyber policy, is worth doing before you need it.

Within that framework: cyber policies typically include funds transfer fraud (someone impersonates the insured to convince a bank to move the insured's

own money), computer fraud (someone breaks into the insured's systems and causes money or securities to be transferred out), and social engineering coverage for the firm's own funds.

Crime insurance, by contrast, includes fraudulent instructions coverage. When a loss touches both coverages, Travelers coordinates the claim across the cyber and crime forms.

"Social engineering in our world means it's our insured's money and not their customer's money. Their customer's money is covered under fraudulent instructions." - Tracey Santor

A real claim illustrates how quickly this can escalate. Two employees at an asset management firm received an email that appeared to come from a customer's CEO, including a signed consent granting power of attorney to a new individual and authorizing that person as a signatory on the customer's account. The firm processed the business authorization certification — which, unbeknownst to them, had been completed by the fraudster, not the customer. Roughly three weeks later, the firm received a follow-up email,

again appearing to be from the CEO, authorizing an \$800,000 transfer out of the account. The transfer was made. Two days later, the real customer called asking why \$800,000 had been moved from her account.

"If a firm grants authority for a new employee to have financial authority without verifying anything, they have just given the crooks the keys to the vault, and the money moves quickly after that." - Tracey Santor

The verification failure, according to Santor, was addressable: any request to add a new signatory or to grant expanded access to financial authority should be confirmed with someone other than the requester — ideally the customer's CFO or another known contact — before that access is granted.

BEST PRACTICE:

Treat any request to add a signatory, grant financial authority, or expand account access with the same scrutiny as a wire transfer request. Verify with someone other than the person requesting the change.

CHAPTER 5

Check Fraud Hasn't Gone Away — It's Gotten Smarter

“They're only acid washing the payee's name off the check. They're not changing the amount; it gives them a longer tail before they get caught.”



Check fraud might seem like an old-fashioned risk in a digital world, but Travelers' claims data tells a different story. Forgery losses surged over roughly the last five years, driven in part by mail theft — fraudsters obtaining or buying “arrow keys” that open the blue collection boxes used by the U.S. Postal Service. This allows them to sift through the mail in search of checks. That trend has begun to decline as postal enforcement has increased and corrective measures have been put in place.

Even though checks aren't being used as often as they have been in the past, they are still out there and provide an opportunity for the fraudsters to steal money. Today, however, the fraudsters have elevated their methods. When they steal a check, they acid wash the payee's name off of the check and replace it with another, typically synthetic identity. Rather than altering the dollar amount on a stolen check — which draws immediate attention when the account is reconciled — fraudsters are only altering the payee's name, leaving the amount untouched. A bookkeeper who reconciles a \$100,000 check that cleared for \$100,000 checks it off the list without noticing the payee changed. The result is a longer window before the fraud is discovered.

"Usually, they're only acid washing the payee's name off the check. They're not changing the amount; it gives them a longer tail before they get caught."

— Tracey Santor

Positive Pay — a bank service that requires the account holder to confirm checks before funds are released — helps close this gap, but only when it includes payee-name verification, which firms typically have to request specifically. Without it, positive pay confirms only the check number and amount, not who the money actually went to.

There is also an important coverage nuance here. Standard forgery coverage under a fidelity bond generally applies only to incoming forgery — a check the firm deposits that is later returned as fraudulent, leaving the firm out of the funds if it already disbursed money against it. Today's fidelity bonds for asset managers do not typically cover outgoing forgery, where the firm's own check is stolen and altered or counterfeited before being cashed. In those cases, if the claim window with the cashing bank has expired, the firm can be left holding the loss. Travelers has a new endorsement in development specifically to extend coverage to outgoing check fraud for asset managers.

Mark Liftman experienced this firsthand: a fraudster produced an almost-exact copy of one of his checks, caught only because a small detail was missing that alerted his bank. He also noted that his bank had stopped including check images on statements — making it harder to catch this kind of fraud during routine reconciliation — and reinstated them only after he filed a claim.

BEST PRACTICE:

Ask your bank specifically to include payee-name verification in your Positive Pay service – it is not automatic, and without it you may not catch the check that only changes the payee name but not the amount of the check.

Confirm whether your fidelity bond covers outgoing check fraud, not just incoming forgery. Ask your Liftman representative about Travelers' new outgoing-check endorsement for asset managers as it becomes available.

Request check images as part of your regular bank statement, not as a manual lookup, so payee names are visible during routine reconciliation.

CHAPTER 6

Real Estate Transactions Are a Favorite Target

“ A verification process can fail even when a firm believes it is doing the right thing. ”



Angela Dennis shared a case that illustrates how a verification process can fail even when a firm believes it is doing the right thing. An asset manager's client was in the process of buying a property, and the client and asset manager had been corresponding back and forth for roughly a week — all of it authentic. At the final step, when it was time to transfer the funds, a fraudster who appeared to have been monitoring the exchange inserted themselves into the process with wiring instructions of their own.

The asset manager did make a callback — but the call confirmed only intent,

not detail: essentially, “Are we a go?” “Yes, we are a go.” The account number, bank name, and dollar amount were never read back or confirmed. Over \$700,000, intended as a deposit on the property, was wired to the fraudster's account instead.

“What he should have said is, ‘do you want it to be transferred to this bank account? These are the numbers... this is the amount’ — and there goes the money.”
— Angela Dennis

The lesson, as Dennis framed it, is that a callback confirming general intent is not the same as verification. A genuine verification call reads back every specific

detail — the receiving bank name, the account number, and the exact dollar amount — and requires the customer to confirm each one aloud.

BEST PRACTICE:

When verifying any wire or transfer, read back the complete details — bank name, account number, and dollar amount — and require the customer to confirm each one. A general “yes, go ahead” confirms nothing.

Build this level of detail into your firm's standard operating procedures and train staff on it explicitly, rather than relying on individual judgment in the moment.

CHAPTER 7

Not Every Firm Carries the Same Coverage — and That's a Risk

“Crime insurance requirements — including the fidelity bond coverage at their core — are not uniform across the financial industry.”



Crime insurance requirements — including the fidelity bond coverage at their core — are not uniform across the financial industry, and that inconsistency creates a real exposure gap for some firms. Broker-dealers are required to carry crime coverage as a condition of doing business. Asset managers are not always subject to the same requirement — which means some firms may be self-insuring risks they haven't fully considered, simply because no regulator requires them to close the gap.

“There's a difference between the broker-dealers and the asset managers...because broker dealers are required to carry the crime coverage where the asset managers aren't always required to carry it. So making sure that they're aware of the risks that are out there and what they may be self-insuring if they don't have this coverage is important.”
- Angela Dennis

Beyond the baseline crime coverage, firms often need additional, activity-specific coverage that many don't realize applies to them. A firm investing in mutual funds needs an investment company blanket bond to comply with the Investment Company Act of 1940. A firm managing pension assets subject to ERISA needs a fiduciary dishonesty bond or a third-party ERISA bond. A broker-dealer needs coverage that complies with FINRA Rule 4360. Customers who the asset managers work with frequently require these coverages directly as a condition of the relationship.

Mark Liftman summarized the underlying principle simply, drawing on something his father used to say: carry coverage that's proportional to your actual exposure – not a minimum limit chosen without reference to what a real claim would cost.

BEST PRACTICE:

Don't assume your current policy covers every applicable requirement. Confirm with your Liftman representative which compliance bonds apply to your specific activities – mutual fund investing, ERISA plan management, or broker-dealer status – and close any gaps.

Review your coverage limits against your actual assets under management and transaction volume, not an arbitrary minimum.

CHAPTER 8

Five Things Every Firm Should Do Right Now

Asked what she would tell Liftman's clients to prioritize above everything else, Santor pointed to five practices that consistently separate firms that catch fraud early from firms that don't.

1) Separate duties wherever possible. No single employee should control bank accounts, invoicing, payroll, and client billing without independent oversight — and where a small staff makes full separation impossible, someone above that function needs to periodically review the activity.

2) Call back every transfer or account -change request to a predetermined phone number — never a number provided in the request itself — before acting on it.

3) Verify complete details, not general intent. Read back the account number, bank name, and dollar amount on every

wire and require explicit confirmation of each.

4) Invest in technology that flags anomalies — tools that can detect an unusual spike in transaction velocity on an account and hold the transaction for review before funds move.

5) Talk to your peers. Fraud that hits a competitor down the street is often headed your way next — sharing what you're seeing, and hearing what others are seeing, helps everyone spot it sooner.

BEST PRACTICE:

Put these five practices into a written, documented procedure — not an informal understanding among staff. Firms that formalize their process typically catch problems faster and recover more of what's lost when something does slip through.

Why Choose Liftman Insurance

Since 1957, Liftman Insurance has been more than a broker — we have been a trusted partner to over 2,500 financial advisory firms and broker-dealers across the country.

Our relationships with carriers like Travelers run deep. When claims like the ones described in this white paper happen, we want to be the call our clients make — the voice advocating for them, and the resource that already understands their specific exposure as an asset manager or broker-dealer, not a generalist explanation after the fact.

Mark Liftman put it simply: *you need a specialist in this area. We have our finger on the pulse every day of what's going on with our advisors, broker-dealers and with the industry. Our carrier partners keep us informed of what they're seeing so we can pass it along before it becomes a problem.*



Mark Liftman
President

Liftman Insurance

This material is for general informational purposes only and is not legal advice. It is not designed to be comprehensive and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or other professional adviser. This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations. Claim scenarios are based on actual claims, composites of actual claims, or hypothetical situations. Resolution amounts are approximations of both actual and anticipated losses and defense costs. Facts may have been changed to protect confidentiality.

Travelers Casualty and Surety Company of America and its property casualty affiliates. One Tower Square, Hartford, CT 06183



Let's Talk About Your Crime/Financial Institution Bond Coverage

Whether you're reviewing an expiring, coverage confirming which compliance coverages apply to your business, or wondering whether your current limits reflect your current exposure — Liftman Insurance can help you navigate these decisions with clarity and confidence.



Call 1-877-LIFTMAN



Visit www.liftman.com



Or connect directly with a Liftman representative to schedule a coverage review.