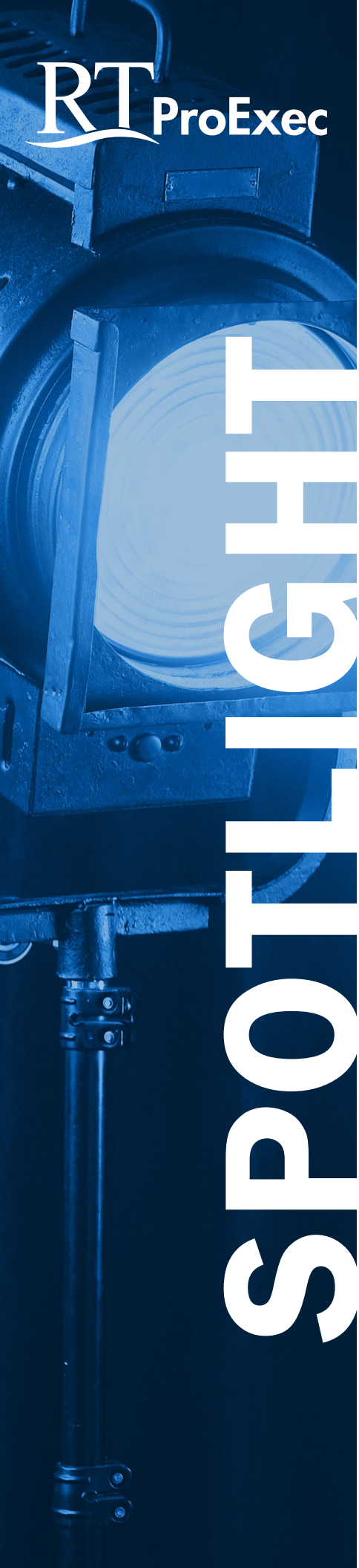

VOLUME 1 – ISSUE 1

CONTACT:
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

Man-in-the-Middle Cyber Exposures Are Growing for Those with Fiduciary Responsibility

You may think you are communicating directly with another individual, but what if someone else is lurking in the network? Man-in-the-middle cyber exposures are growing, and the resulting losses are not always covered under professional liability or cyber insurance policies. Any company with fiduciary responsibilities should review their policies and consider implementing appropriate risk management practices to take control of this tricky exposure.

The Man-In-The-Middle Risk

In man-in-the-middle attacks, hackers infiltrate two-party communications. In some attacks, the hackers do this in order to steal sensitive information, such as credit card numbers, acting as silent spies in your network. In other attacks, the hackers actively send or alter messages for their own gain. These attacks are similar to business email compromise schemes, but they are even more insidious because they piggyback on legitimate communications.

MAN-IN-THE-MIDDLE ATTACKS AREN'T JUST A PROBLEM FOR REAL ESTATE FIRMS. THEY CAN TARGET LAW FIRMS, INVESTMENT COMPANIES OR ANY OTHER INDUSTRY IN WHICH COMMUNICATIONS MAY INCLUDE SENSITIVE FINANCIAL INFORMATION AND WIRE TRANSFER INSTRUCTIONS.

The losses can be both significant and irrecoverable. For instance, Check Point Research reports a man-in-the-middle attack resulted in $1 million being stolen, when a Chinese venture capital firm attempted to send funds to an Israeli startup. When the startup never received the seed funding, the two parties investigated and realized that the emails between the two parties had been modified, and completely fabricated by an unknown third party. Hackers had infiltrated their communications.

Many Industries Are At Risk

Man-in-the-middle attacks have frequently targeted the real estate industry. Imagine a real estate transaction where the proceeds must be sent to the seller at closing. In this scenario, the seller's attorney retrieves the wire instructions from a secure portal and then verifies those instructions directly with the sender to ensure accuracy and security.

FBI Internet Crime Complaint Center (IC3) reports that real estate-related losses reached $173.5 million in 2024 with business email compromise (BEC) topping $2.7 billion.

However, man-in-the-middle attacks are not just a problem for real estate firms. They can target law firms, investment companies or any other industry in which communications may include sensitive financial information and wire transfer instructions.

How You Can Be Held Liable

Although it may seem unfair, if a hacker targets a client's sensitive communications, you could be held liable for failing to uphold their fiduciary responsibility. To make matters worse, you may not have coverage under existing insurance policies that extends to this loss.

Consider an attack scenario involving a defense attorney whose client lost a case.

- An escrow agent was holding funds pending the case outcome.
- Once the defendant was ordered to pay, payment instructions were sent to the defense attorney.
- The defense attorney forwarded the instructions to the escrow agent.
- The escrow agent then released the funds without taking any additional steps to verify the payment instructions.

The firm subsequently received an email from the sender advising of new payment instructions. This email was forwarded to the closing agent without further verification. The closing agent asked the law firm, if the instructions had been verified, and the law firm erroneously confirmed that they were. So, without any further verification from the original sender, the closing agent released the funds—straight into the hacker's account.

Scams may target anyone involved in a real estate transaction, including buyers, sellers, attorneys, title companies and agents. It was discovered that the original instructions were altered and that the defense attorney was the target of a man-in-the-middle attack. The plaintiff's attorney, who originally sent the instructions, had been compromised. Who was to blame—the plaintiff attorney whose systems were compromised? The defense attorney who merely passed along the instructions and was not holding or dispersing any funds? Or, perhaps, the escrow agent?

Update to Man-in-the-Middle Cyber Exposures

There were failures at every point in the process. The plaintiff law firm failed to secure its systems against intrusion, the defense law firm failed to verify the instructions before forwarding them to the escrow agent, and the escrow agent failed to verify the instructions before releasing funds.

The defense law firm reported the incident to its **cyber insurer**, but the claim was denied, stating the firm never had control of the funds and did not release the funds, so the social engineering coverage in the policy was not triggered.

The defense law firm's **professional liability policy** did not provide coverage either. Although some professional liability policies may provide coverage on the basis that failing to validate the instructions before sending to the escrow agent amounts to professional negligence, the policy had a strict exclusion that barred coverage for social engineering losses.

In the end, the escrow agent was held liable for the loss as the one who directed the wire transfer without verifying it first, but everyone involved incurred fees and lost time before this crisis was resolved.

SAFEGUARDING AGAINST WIRE TRANSFER FRAUD

Even if you're working with people you trust, implementing strong security measures is important because you never know who may be intercepting and altering your messages.

STRONG SECURITY MEASURES IS IMPORTANT BECAUSE YOU NEVER KNOW WHO MAY BE INTERCEPTING AND ALTERING YOUR MESSAGES.

A few best practices to consider are:

- **Verify wire transfer instructions.** Use a different method of communication to verify instructions. For example, if new instructions were sent by email, call a known, valid number (not one noted in the email) to confirm their validity. This should be done whether you are the party directing the transfer or you are sharing the information with another party who will direct the transfer.
- **Be especially cautious when new or altered instructions are received.** This is a common tactic used by scammers. If someone says they've switched accounts, be sure to verify the account number using a secure method.
- **Don't rush.** Scammers often create a false sense of urgency to trick victims into skipping verification processes. Although you may have deadlines to consider, it's critical to ensure the transfer instructions are accurate.
- **Don't rely on someone else's word.** Instead of asking if the information has been verified, verify it yourself.

REVIEW YOUR INSURANCE COVERAGE

Man-in-the-middle attacks often occupy a coverage gray area. Although they're often lumped with cyberattacks, they may not meet the criteria of an insured cyberattack under insurance policy definitions.

A few considerations when evaluating a cyber policy:

- **Does the cyber policy require a verification process?** Cyber policies often require that strong security measures be put in place, and failure to do so could jeopardize coverage.
- **Does the cyber policy cover funds in an escrow account?** If the insured must have control of the funds to trigger coverage, incidents involving funds in escrow could be excluded.
- **Does the professional liability policy exclude social engineering losses?** Many do, while others are silent on the matter, and some offer coverage but with a lower sub-limit. Although it may seem counterintuitive, policies that are silent on the matter may provide the most coverage.

THE BOTTOM LINE

Insurance agents can add value for their clients by discussing man-in-the-middle risks and related coverage with their clients. Professionals who are involved in financial transactions— even if they don't hold or release funds themselves—can help protect themselves with strong security practices and thoughtfully considering their coverage options.

Have questions? Need help structuring coverage? Reach out to the RT ProExec team for assistance.

The RT ProExec Advantage

RT ProExec is a leading specialty insurance practice focused exclusively on Executive, Professional and Transactional Liability. We provide cutting-edge product knowledge, innovative placement methodologies, and exceptional service to support retail clients and their insureds.

Why should you collaborate with us?

We help our retail trading partners retain existing clients, win new prospects, and grow their portfolios. While expert assistance from a wholesale broker can provide a notable competitive advantage anytime, it is particularly crucial during disrupted markets.

RT ProExec delivers market leading scale and depth.

- Dedicated industry verticals
- Proprietary and exclusive products and enhancements
- Creative problem-solving
- Robust educational resources and services
- Claims advocacy and support