MARSH

INSIGHTS | JANUARY 2020

Tech-Enabled Fraud: Addressing Insurance Coverage Pitfalls in Third-Party Attacks

Bad actors are continuously looking for weak links to exploit in financial ecosystems. With cybercrime on the rise and attacks on third parties a reality that financial entities must prepare for, finding ways to protect their assets from insurance coverage pitfalls is essential.

But this isn't always easy or straightforward. Financial institutions and vendors that provide financial services to these institutions often have interdependent business operations, which can make it challenging to determine whose insurance and what type of coverage will respond to an impersonation fraud event targeted at asset managers, custodians, administrators, and their clients.

When Coverage is Disputed

This challenge has been brought to the forefront as a fund administrator seeks indemnification in a declaratory action against its insurer. The case stems from recently settled litigation between SS&C Technologies, a fund administrator, and Tillage Commodities Fund, a hedge fund client, involving a $5.9 million impersonation fraud scam.

In 2016, Tillage filed a complaint alleging breach of contract and breach of implied covenant of good faith and fair dealing against SS&C in the New York State Supreme Court. Earlier that year, an SS&C employee received six emails containing instructions to transfer funds totaling $5.9 million from Tillage's account, over which SS&C had transfer authority, to an HSBC account in Hong Kong. Although the emails purportedly came from Tillage, they were in fact from a spoofed email domain that misspelled the company name (as "Tilllage"). The employee followed the instructions and wired the requested funds each time.

The action alleged breach of contract, claiming that SS&C did not follow protocols established in its contract with Tillage, including the use of a filtering tool on all incoming emails. The action also alleged breach of implied covenant of good faith and fair dealing, claiming that SS&C ignored both its own stated practices and basic procedures recommended by the FBI, such as not using the "reply" button to respond to emails requesting funds transfers. In June of 2019, Tillage and SS&C settled these claims on a confidential basis with no admission of wrongdoing by either party.

SS&C's Case for Coverage

SS&C's cyber/errors and omissions (E&O) policy contained a professional liability insuring agreement that provided coverage for losses resulting from claims against the fund administrator due to any negligent act, error or omission, misstatement, or misleading statement in its performance of professional services. As such, SS&C tendered the Tillage lawsuit to its insurer for defense and indemnity.

While the insurer acknowledged that the suit falls within the provisions of the professional liability coverage section and has agreed to pay related defense costs, it has denied coverage for indemnification, citing several exclusions. These include:

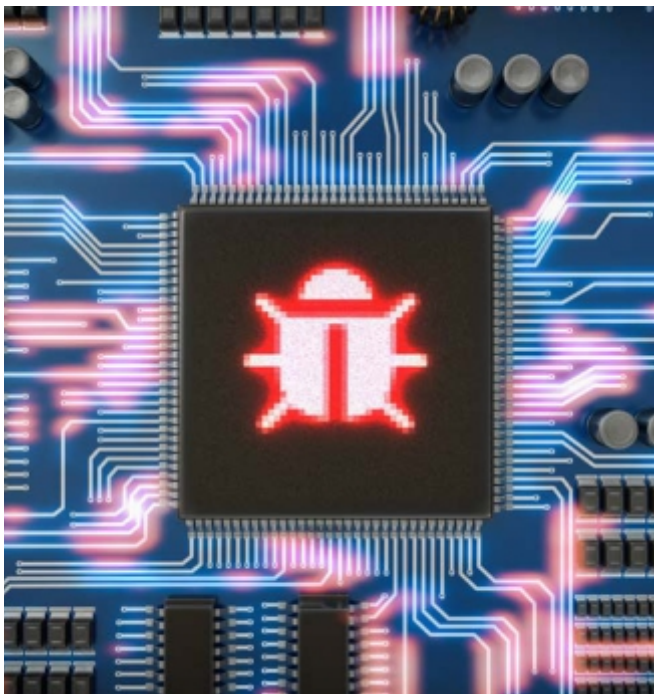
- A conduct exclusion, which is being disputed by SS&C because it requires final adjudication by the court, which has not yet occurred.
- An exclusion for the monetary value of a transaction from an insured's account. SS&C is arguing that this exclusion is not applicable since the funds were wired from Tillage's account, and not SS&C's.
- An exclusion for loss arising out of SS&C exercising authority or discretionary control over client funds. SS&C is arguing that this exclusion is inapplicable for two reasons: because SS&C did not have discretionary authority over Tillage's funds, and because a provision within the exclusion states that it does not apply to any claim arising out of SS&C's performance of professional services.

Mitigation Steps for Financial Entities

This case is still making its way through court. But even as we wait for the final outcome, there are some key observations based on current information.

First, SS&C had a tailored cyber/E&O policy that contemplated coverage for negligence in its performance of professional services. While many financial services firms procure their own professional indemnity insurance coverage, they should also purchase robust fidelity/crime policies that cover them in the event they transfer customer funds based upon fraudulent instructions.

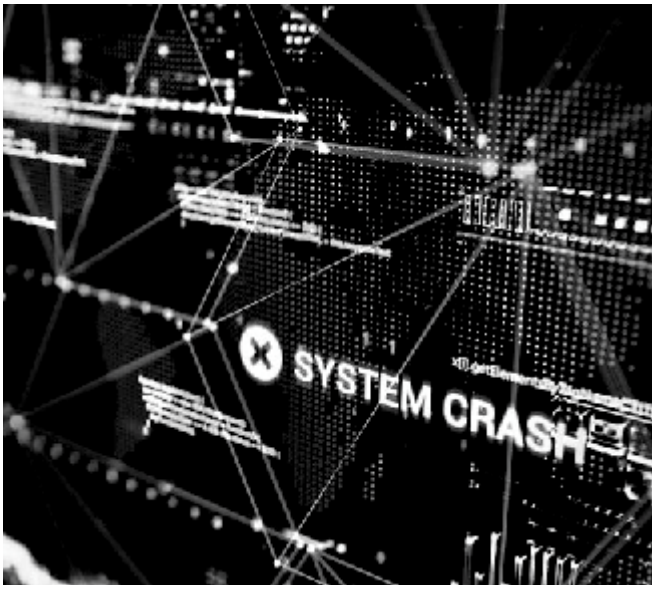
Simultaneously, a financial institution that entrusts control of its accounts or funds to a third party should contractually require that the company carries not only a comprehensive E&O policy, but also a crime policy/fidelity bond that includes impersonation fraud and funds transfer fraud coverage (with no conditions precedent to liability). These financial institutions should also be added as joint loss payees on their financial services firms' policies. Additionally, financial institutions should require that the accounts and/or funds that are entrusted to third parties are considered covered property under the third party's crime policy/fidelity bond.



Finally, to avoid relying solely on a third party's solvency or insurance for risk transfer, financial institutions may seek to amend the definition of employee in their own crime policies/fidelity bonds so that a fund administrator is deemed an employee, at a minimum for the purposes of employee dishonesty, impersonation fraud, and funds transfer coverages.

Ensuring Effective Coverage

Losses from technology-enabled fraud can be substantial and involve more than one organization. Financial institutions should take a close look at any relevant policies they and their vendors purchase, paying close attention to the policies' language to ensure they provide appropriate coverage for otherwise covered losses caused by technology-enabled fraud. Risk professionals should also work closely with their brokers and insurers to identify – and address – potential coverage gaps and exclusions and make certain that all relevant policies are aligned.



About Marsh's Financial Institutions FINPRO Center of Excellence

Marsh's Financial Institutions FINPRO Center of Excellence is committed to developing risk solutions and services to help you manage your critical risks and ultimately make you more successful. We serve more than 7,000 financial institutions globally, and creativity, innovation, and ongoing investment in analytics are our hallmarks. Across all sectors of the financial industry, we can deliver technical expertise, knowledge of legal and regulatory trends, specialized claims advocacy services, and deep access to insurers — all to help you develop and implement a risk management program tailored to your risk issues.

For further information on Marsh's cyber insurance solutions, visit marsh.com, send an email to cyber.risk@marsh.com, or contact your Marsh representative.

SIMON BELL
Financial & Professional Lines
Leader - MENA
+971 50 450 1935
simon.bell@marsh.com

TALAL Y. DARRAS
Business Resilience Leader -
MENA
+971 56 174 0379
talal.darras@marsh.com