Paragon

EXECUTIVE RISKS

THE WIRECARD STORY:

HOW DOES FINTECH INSURANCE INDEMNIFY IN THE EVENT OF FRAUD?

WHITEPAPER

August 2020

Contents

Introduction	**3**
Directors' & Officers' Insurance	**4**
Professional Liability Insurance	**6**
Cyber Insurance	**8**
Crime Insurance	**10**
Key Takeouts	**12**
About Paragon	**13**
Speak directly to our senior Fintech brokers	**14**

After admitting that €1.9 billion was "missing", Wirecard AG ('Wirecard'), one of the world's fastest growing digital payment platforms and an iconic Fintech brand, came crashing down. The admission of fraud saw the downfall of one of Germany's most revered companies, which in 2019 boasted 5,800 employees in 26 locations and a market value that exceeded that of Deutsche Bank.

A special audit by KPMG in April 2020 confirmed that dubious accounting methods had been used to overstate revenue, documents had been forged to show the existence of €1.9 billion allegedly held in bank accounts in the Philippines and these documents had been used to mislead auditors and investors of Wirecard.

The Wirecard scandal has resulted in Germany's financial services regulator, BaFin, commencing an investigation and the arrest of Wirecard's CEO. Germany's Finance Minister has also increased BaFin's investigative authority to that of "sovereign powers". It can be expected that scrutiny by financial regulators in all key Fintech hubs, including the UK Financial Conduct Authority, US Securities Exchange Commission and Consumer Finance Protection Bureau, Australian Securities and Investment Commission and Monetary Authority of Singapore will likely follow. Therefore, it is important that executives of Fintech companies review their insurance for cover against regulatory investigations involving directors and officers and the company's costs incurred in responding to and defending regulatory actions.

Paragon's Fintech insurance policy covers companies for Directors' and Officers' insurance, Employment Practices Liability insurance, Professional Liability insurance, Cyber insurance and Crime insurance. It covers companies and executives who may find themselves in circumstances involving legal claims alleging a breach of duty, regulatory investigations, shareholder claims, employee claims, customer claims, cyber breaches and employee theft. The events of Wirecard highlight the value of a Fintech insurance policy and can be used to show how a Fintech insurance policy would indemnify a company and its executives against various legal claims.

For advice on the type of Fintech insurance policies suitable for your company, please contact our specialist team.

Best regards,

Rhys James

Partner and Head of Executive Risks, Paragon International Insurance Brokers

Directors' & Officers' Insurance

Once a quarter, each partner (company) emailed statements to Wirecard that outlined "credit card transactions processed in the respective periods and the commissions subsequently due". KPMG said that on the basis of those emailed spreadsheets, Wirecard booked revenues and costs.

Source: Financial Times

Directors' & Officers' insurance (D&O) has two primary objectives. Firstly, to pay legal defence costs and any settlement or judgements awarded against any directors or officers of a company when the company has failed to indemnify the directors and officers for such expenses they incurred. Such failure typically occurs in the event of insolvency or shareholder derivative litigation where the company is prohibited from indemnifying the directors or officers. Secondly, to pay on behalf of the company any legal defence costs and any settlement or judgements incurred as a result of a duty to indemnify a director or officer, or for shareholder claims made directly against the company.

The value of having a D&O policy in place is that it allows a company to attract and maintain a high-quality board and executive team. A D&O policy will provide comfort to these executives that they are protected should any legal claims be made that name individual directors or officers in a complaint, or there is a regulatory investigation requiring the executive to prepare and respond to questioning. A D&O policy is also important as an appropriate hedge on a company's balance sheet against costly litigation. Proper due diligence should be undertaken on the scope and amount of D&O required.

What is covered?

A D&O policy will trigger upon any actual or alleged act, error, omission or breach of duty by any director or officer while acting in his or her managerial capacity. In the case of Wirecard, the allegation that Wirecard's accounting controls were not sufficient to "fully ascertain the amount and existence of the revenues" (KPMG) would have triggered the policy. This is because the accounting controls would be considered a "Wrongful Act" within the scope of a D&O policy and accordingly any legal action or regulatory investigations against directors or officers that flowed from this wrongful act would be covered by the policy.

Directors' & Officers' Insurance (cont.)

What is excluded?

Three important exclusions to understand include:

- **Fraud.** It is important to understand that any intentional fraud or criminal act by a director or officer is excluded from a D&O policy. However, there is scope to negotiate when such conduct is deemed excluded from cover, for example, if the fraudulent conduct can only be determined after a final adjudication, then an insurer will advance all defence costs until such time.
- **Employment Claims.** Claims arising against a company for an actual or alleged act or omission, breach of statutory provision or breach of common law relating to an employee are typically excluded from a D&O policy. This cover is procured under a separate policy called Employment Practices Liability insurance (EPL). An EPL policy would cover claims for such wrongful acts, including failure to provide equal opportunity of employment or pay, discrimination, harassment (sexual or otherwise) and wrongful dismissal or treatment.
- **Services to customers.** Legal claims made against a company which arise out of services provided to customers are generally excluded from a D&O policy. Cover would typically be provided for individual directors or officers when allegations against them relate to their managerial capacity, but claims against the company would be excluded. This is because this risk is separately insured in a Professional Liability insurance ("PL") policy, also known as a Professional Indemnity (PI), Errors & Omissions (E&O) or Civil Liability insurance policy. The importance of a PL policy for Fintech companies is discussed below.

Professional Liability Insurance

In 2017 Wirecard claimed publicly to serve 33,000 large and medium-sized merchants, and 170,000 small businesses, a global reach that helped make the company an investment sensation.

Source: Financial Times

Fintech companies owe a duty to their customers. Legal claims can arise from any allegation of any act, error, omission or breach of such duty by a company in the performance of services to customers.

PL provides indemnity for legal defence costs and any settlement or judgements against a company for an alleged wrongful act in the provision of services to others. The cover is specific to the nature of the operating activities. For example, if the services are Professional, Financial or Technology in nature the policy will reflect this. Fintech companies need to ensure that the scope of services covered is appropriate for their activities.

Fintech companies should consider PL that is tailored to the type of services provided, for example, payments, lending, investments, capital markets, insurtech or digital assets. Appropriate PL will help Fintech companies protect their balance sheet against the risk of expensive litigation arising from customers because of an alleged wrongful act or complaint.

What is covered?

A PL policy will cover legal defence costs and any settlement or judgements against a company for an alleged wrongful act in the performance of Professional, Financial or Technology services to customers.

Cover can also be available for the costs incurred to respond and defend an investigation by a regulatory body into an alleged wrongful act by a company in the performance of Professional, Financial or Technology services to customers.

Professional Liability Insurance (cont.)

What is excluded?

Two important exclusions to understand include:

- **Fraud.** It is important to understand that any intentional fraud or criminal act is excluded from PL policies. However, there is scope to negotiate whose conduct is imputed on a company when assessing coverage for fraud. Good standard policies will not assert that the conduct of one person is imputed to any other persons and that only the conduct of senior managers, for example CEO or CFO, would be imputed to the company. This is important when assessing the risk of fraud by employees on customers. As with a D&O policy, there is scope to negotiate when such conduct is deemed excluded.
- **Contractual Liability**. This is an important exclusion in a Fintech policy as most services to customers are governed by contract. The exclusion seeks to avoid the insurer paying for liability expressly accepted in customer contacts. However, cover is commonly carved-back for liability that would have existed in the absence of such contact. The exclusion seeks to avoid contractual penalties, liquidated damages or any similar guarantee or warranty.

Cyber Insurance

"Wirecard AG has at no time been in direct or indirect contact with a hacker group from India."

Source: Financial Times

The Wirecard scandal brings into focus the ubiquitous nature of cybercrime in 2020. Wirecard is alleged to have targeted critics of the company, including short sellers, journalists and investigators with hacker-for-hire group Dark Basin.

While Wirecard was not itself the subject of a cyber-attack, many companies are and in 2020 these attacks have included the ransomware attack on Finstra, Robinhood's system outage, EasyJet data breach and the hack of Twitter. Each of these examples illuminates the vulnerability of well-guarded technology systems and the consequential risk to business.

What is covered?

Cyber insurance improves a Fintech company's cyber resilience by providing indemnity in the following six key areas:

- **Data Breach and Network Security Liability -** the insurer will pay the legal defence costs and any settlement or judgements against a company for an alleged loss, theft or failure to protect personal data or for the failure to prevent a cyber security breach.
- **Privacy Regulatory Defence, Awards and Fines -** the insurer will pay the legal defence costs and any civil monetary fine or penalty imposed by a regulatory authority. The payment of such fines by insurers is precluded if the matter is deemed uninsurable under the law pursuant to which the policy is construed (see what is excluded on the next page).
- **Business Interruption and Extra Expense -** the insurer will pay for loss of business income and reimburse a company for extra expense during the "period of restoration", which is typically between three to six months, that the company incurs resulting from a cyber security breach.
- **Data Recovery -** the insurer will pay reasonable and necessary costs incurred to determine whether damaged or destroyed data can be replaced or repaired, and replace or repair such damaged or destroyed data.
- **Cyber Extortion -** the insurer will pay money or property under duress for the purposes of preventing or terminating a cyber extortion or ransomware threat and reasonable expenses incurred for a security consultant to prevent, mitigate or terminate a cyber extortion or threat.

Cyber Insurance (cont.)

- **Data Breach Response and Crisis Management Costs -** most Cyber insurance policies will include a "Breach Response Panel", and a company will be authorised to engage an expert panel of legal and computer forensic service providers to respond to the cyber security event at the Insurer's cost. Such assistance can include determining the legal actions necessary to respond to data breach reporting requirements, performing computer forensics to determine the cause and scope of a cyber security breach, notifying individuals of a data breach who are required to (or should otherwise voluntarily) be notified, operating a call centre to manage data breach inquiries, providing credit or identity protection services and minimising harm to a company's reputation by hiring a public relations or crisis communications firm.

What is excluded?

Two important exclusions to understand include:

- **Fraud, other than a "Rogue Employee".** Intentionally dishonest, fraudulent or criminal acts are excluded, unless such acts are committed by a rogue employee. Typically defined as an employee who deliberately acts outside the course of employment and whose intentional conduct results in a cyber security event. Notably most policies will preclude the actions of a company's executive officers for the cover granted for rogue employees.
- **Fines & Penalties deemed uninsurable by law.** Introduction of the General Data Protection Regulation (GDPR) brought into sharp focus the insurability of regulatory fines and penalties following a data breach, under which the supervising authorities (Information Commissioner's Office in the UK) have increased authority to impose fines. It should be noted that the UK authorities have not declared whether or not any fines they issue should be capable of being insured, unlike the Financial Conduct Authority (FCA) in the UK, which expressly prohibits the insuring of fines it imposes for breaches of financial regulations. Fines flowing from criminal conduct will not be insurable as it is clearly against public policy for fines resulting from reckless criminal wrongdoing to be indemnifiable. How administrative fines under the GDPR will be addressed is less clear. However, insurance will still play a part responding as it may do to investigation costs, defence costs and breach response costs.

Crime Insurance

"It's really something that caught us by surprise... when EY gave us a copy of that document to verify, we immediately realised it was bogus - it was falsified." BPI president and chief executive.

Source: Financial Times

The 'oh...!' moment when directors and officers identify a financial crime within their company is personally and professionally critical. Crime insurance protects a company against criminal behaviour of a dishonest employee or a dishonest third party, including collusion between the two.

Fintech companies often have unique vulnerabilities including periods of high employee growth following successful funding rounds, large volume fund transfers, multi-national officers and digital assets. It is important that reasonable due diligence is undertaken on the potential loss from employee or third-party crime and the value of insurance.

What is covered?

Broadly Crime insurance will indemnify an insured company for loss of money, securities or other property resulting from:

- employee theft, including collusion with a third party;
- computer and funds transfer fraud, covering loss of money from fraudulent entry of computer programmes or funds transfer resulting from fraudulent phishing or social engineering fraud;
- forgery or alteration; and
- theft of money, securities or property inside a company's premises or a financial institution's premises.
- Theft of digital asset private keys and the fraudulent transfer of cryptocurrencies can also be insured with bespoke risk underwriting and on specialist policies.

Crime Insurance (cont.)

What is excluded?

Some important exclusions to consider are:

- consequential or indirect losses, such as lost profits from reputational damage;
- losses occurring after such time an executive officer (not in collusion) has knowledge;
- theft or fraud by a major shareholder;
- intellectual property theft including copyright, customer information, patents, trademarks or trade secrets; and
- trading losses, unless such loss results in an employee making improper financial gain for themselves or for any other individual or organisation intended by such employee to receive such benefit.

Key Takeouts

There are many lessons to be learnt from the Wirecard story. This case study illustrates the risks that materialised at Wirecard and the relevant insurance options that would have been available for them under a Fintech insurance policy.

Not all events are as dramatic as Wirecard. However, executives of companies of all stages - start-up, to growth stage and public companies - need to consider how to implement an effective cadence of corporate governance and, as part of this, regularly question: how effective is my insurance programme?

An appropriate answer to this should consider the following insurance options:

- **D&O** which indemnifies the board and executives for personal liability and a company against shareholder claims. Employment claims are separately insured in an EPL Policy.
- **PL** which indemnifies a company for defence costs, settlement or judgements against the company for an alleged wrongful act in the performance of Professional, Financial or Technology Services to customers.
- **Cyber insurance** which can improve a company's cyber resilience by providing indemnity in the following six key areas: data breach and network security liability; privacy regulatory defence, awards and fines; business interruption and extra expense; data recovery; cyber extortion; and, data breach response and crisis management costs.
- **Crime insurance** which indemnifies a company against theft of money, securities or other property by a dishonest employee or a dishonest third party.

From an insurance perspective, the key learning from the Wirecard case study is how each element of a Fintech insurance policy will indemnify a company against various legal claims. Of important consideration is the scope of claims that can be made against a company in the event of fraud, including shareholder claims, regulatory claims, customer claims. Further, to understand your insurance cover it is important to consider how, and when, any fraud exclusions in a Fintech insurance policy will be applied.

Paragon can help Fintech companies by advising on the different types of insurance policies to design bespoke cover, consider what level of insurance to purchase, prepare for insurer presentations, set clear service timelines and negotiate the most favourable premium and policy terms. If your company can present to insurers a strong corporate governance culture, premiums and policy terms will be more favourable.

About Paragon

Paragon is a specialist insurance broker, operating in the Lloyd's of London, Bermuda, European and International Specialty markets. We have market-leading capabilities and experience in the Financial, Professional and Casualty Lines sectors.

With a broad, independent platform, we can deliver the best services and resources for our clients and broker partners, who we partner with, to deliver risk transfer solutions, claims advocacy and risk management services. Our bespoke, highly-personalised approach is unique in the insurance industry.

About Paragon Executive Risks Team:

We are an experienced, results driven team focused on three specialty practice areas:

- public company Directors' & Officers' Liability insurance;
- financial institution Management & Professional Liability insurance; and
- Financial Technology Services Liability, Cyber and Crime insurance.

This focus has led to a clear and concise understanding of the legal, regulatory and board-level risks facing mid-size and large, global organisations. Our clients include Fortune 500, Fintech 250 and multinational organisations. We relentlessly pursue our clients' best interests by listening to challenges and combining technical know-how with hands-on market negotiation.

Speak directly to our senior Fintech brokers

For more information, please contact:

Rhys James
Partner & Head of Executive Risks
E rjames@paragonbrokers.com
T +44 (0)20 7280 8244
M +44 (0)78 7299 4743

William Wright
Partner
E wwright@paragonbrokers.com
T +44 (0)20 7280 8252
M +44 (0)79 0096 8894

Spenser Lee
Partner & Director
E slee@paragonbrokers.com
T +44 (0)20 7280 8205
M +44 (0)77 9230 7386

Jeff Hanson
Senior Vice President
E jhanson@paragonbrokers.com
T +44 (0)20 7280 8286
M +44 (0)77 1189 9888

Ed Ventham
Client Executive
E eventham@paragonbrokers.com
T +44 (0)20 7280 8246
M +44 (0)78 3742 1569