Spotlight 06/26

TOO GOOD A DEAL TO BE TRUE? CRIMINAL CONSEQUENCES OF INVESTMENTS

Wenger Vieli Ltd.
Dufourstr. 56
P.O. Box
8034 Zurich
—
Metallstr. 9
P.O. Box
6302 Zug
—
+41 58 958 58 58
spotlight@
wengervieli.ch

Banks and Financial Service Providers | Capital Market and Listed Companies | **Competition** | Compliance | Construction and Real Estate | Corporate and Commercial Law | Data Protection | Energy | Financing | FinTech | Foundations | Funds and Asset Management | Insurance | Intellectual Property Law | **Internal and Regulatory Investigations** | Labor and Employment Law | Litigation and Arbitration | Mergers and Acquisitions | Migration | Notarial Services | Pharma and Health Care | Private Clients and Estate Planning | Private Equity | Public Procurement | Restructuring and Insolvency | Taxation | Technology and Media | Venture Capital | **White Collar Crime** | Sports Desk | Start-up Desk |

Anyone who invests in a company before insider information becomes public stands to profit—but may also be committing a crime. However, not every information advantage constitutes a criminal offense. The line between a permissible information advantage and a criminal insider transaction is finer than expected.

Insider trading is among the most difficult economic crimes to prove. An information advantage is typically concealed and difficult for the other party to detect. Nevertheless, acting on the basis of an information advantage leaves traces. Anyone who believes that a discreet transaction will go unnoticed underestimates the capabilities of modern market surveillance or the authorities' increased willingness to prosecute. In its 2025 Activity Report, published in April 2026, the Office of the Attorney General also states that a key focus of its criminal prosecution efforts in the area of general economic crime is insider trading, committed by both individuals and organized "insider rings." This increasing trend toward prosecution is also evident in cases involving the exploitation of an information advantage at privately held companies.

This Spotlight examines two key risk areas: insider trading under financial market law pursuant to Art. 154 of the Financial Market Infrastructure Act (FinMIA) for publicly traded companies, and breach of fiduciary duty pursuant to Art. 158 of the Swiss Criminal Code (StGB) in private transactions. It illustrates where the line is drawn between permissible conduct and criminal insider trading—and what companies, corporate bodies, and advisors should take away from this.

Scope of application: what is covered—and what is not

The insider trading offense under financial market law pursuant to Art. 154 of the Financial Market Infrastructure Act (FinMIA) applies to anyone who, as an insider, buys or sells securities by taking advantage of insider information. The penalty may, under certain circumstances, include up to five years of imprisonment. For primary insiders (e.g., members of the board of directors, C-level management, anchor shareholders, etc.), the disclosure of insider information is also a criminal offense. The decisive factor here is first and foremost whether the security in question is one covered by the law.

Listed stocks, derivatives, and other structured products are at the core of insider trading law. It is largely unknown that, since the introduction of the DLT Act, tokenized securities and certain crypto assets may also fall within its scope, provided they qualify as securities. The primary factor determining the application of financial market criminal law is whether the insider information concerns a listed company or publicly traded securities. If this is not the case, criminal liability for a classic insider trading offense is ruled out from the outset.

On the other hand, anyone who acquires or disposes of shares in an unlisted GmbH or AG falls outside the scope of insider trading under financial market law. This applies regardless of what information is available in the process. The insider trading provision of the FinMIA is aimed at safeguarding the integrity of the organized capital market, not at regulating private transactions between shareholders or investors.

However, this does not mean that there are no criminal liability concerns in transactions involving privately held companies. Any member of the board of directors, managing director, employee, or trustee who acts to the detriment of the company or its owners by exploiting an information advantage may be guilty of breach of trust under Art. 158 of the Swiss Criminal Code (StGB). A typical example: An investment manager of a private equity fund is aware of an upcoming major investment by his fund in a portfolio company. Before the transaction is completed, he privately acquires shares in the same company. The resulting increase in valuation dilutes the fund's subsequent stake and harms his employer. The investment manager is acting in his own interest and may thereby have breached his fiduciary duty to his employer and committed a criminal offense under Article 158 of the Swiss Criminal Code (StGB).

In addition, the (paid) disclosure of such information to a third party seeking to carry out a transaction or investment may also constitute a criminal offense. A criminal act of (passive) private bribery appears possible if an undue advantage was accepted in exchange for disclosing the information. Violations of trade secret protection laws also appear possible, such as the breach of manufacturing and trade secrets, provided that the disclosed information constitutes a trade secret. In this case, the acquirer and prospective investor would also be liable to prosecution—for incitement to breach a trade secret.

The lack of a stock exchange listing therefore provides protection against insider trading laws, but not against criminal liability in general.

«AN INFORMATION ADVANTAGE IS A BENEFIT—BUT FROM A CRIMINAL LAW PERSPECTIVE, IT CAN BECOME A LIABILITY.»

Typical risk scenarios

In practice, insider risks rarely arise from deliberate criminal acts. More often, they stem from situations in which the line between permissible conduct and a criminal insider transaction becomes blurred in everyday business, presenting an opportunity that is too tempting to ignore.

In financial market criminal law, M&A processes are the classic high-risk area. Anyone involved in a transaction—whether as an advisor, financing partner, or employee of the target company—regularly gains early access to price-sensitive information. Trades made during such a phase—regardless of the motives—may constitute an insider trading offense. The fact that the information "will become public soon anyway" does not change this. As soon as an advantage over the open market is exploited, the threshold for an insider trading offense may be crossed.

Members of the board of directors and executive management of a publicly traded company are in a unique position in that they are structurally privy to the company's flow of information. Against this back-drop, conflicts of interest may arise that prohibit transactions during certain blackout periods. A typical example: A member of the board of directors of a publicly traded company learns during a meeting of an impending drop in profits. Even before the ad hoc announcement is published, he sells shares of the company that he holds privately. The fact that, as a member of the board, he had structural access to this information establishes his status as an insider and, consequently, his criminal liability. Such risks must be addressed separately.

Finally, the network of advisors also poses risks. Lawyers, auditors, communications consultants, and other external service providers gain access to non-public information as part of their mandates. They, too, are subject to insider trading laws if they receive information about publicly traded companies. Exploiting or disclosing this information may constitute a criminal offense.

The risk associated with privately held companies is largely underestimated. Here, the concept of "front-running" has become established: Anyone who knows that an investment in a privately held company is imminent and invests themselves to profit from the expected increase in value may, under certain circumstances, be guilty of breach of fiduciary duty. Criminal liability may arise from the exploitation of any information advantage: It does not necessarily have to involve an investment by a new major investor; successful research results or strong sales figures, for example, can also be exploited. If this results in damage to the principal of the front-runner, criminal liability may arise. Back-running or tailgating, occurring in the reverse chronological order, also carries the same criminal risks.

Best practices for avoiding criminal liability risks

Criminal risks associated with information advantages are real. However, these risks can be addressed through clear internal processes and the cultivation of risk awareness. Depending on whether the transactions involve publicly traded or privately held companies, different measures are appropriate:

Publicly traded companies:

- Implementation and adherence to clear trading policies (insider regulations) with defined blackout periods.
- Maintaining and regularly updating an insider list; raising awareness among all listed individuals regarding their obligations through training.
- Refraining from transactions during ongoing M&A processes.
- Seeking legal advice at an early stage in cases of uncertainty regarding insider status or whether information is price-sensitive.
- Clear confidentiality agreements with external advisors, including an explicit reference to insider restrictions.
- Comply with reporting obligations to the operator of the financial market infrastructure (e.g., SIX Exchange Regulation).

Privately held companies:

- Raise management's awareness of front-running and back-running risks in the context of financing rounds and M&A transactions.
- Incorporate conflict-of-interest provisions into employment and engagement agreements; issue corresponding employer directives or organizational regulations.
- Assess the criminal law implications before disclosing confidential corporate information to third parties.
- Seek legal advice early on if there is uncertainty regarding fiduciary duties and the risk of causing harm.

An information advantage can be a benefit. Under criminal law, it becomes a liability if it is used for personal gain. The risk begins sooner than most people expect.

Keyfacts

01 Insider trading does not just affect stock market professionals. Anyone with access to non-public information about publicly traded companies can be subject to criminal prosecution—regardless of their official role.

02 The lack of a stock exchange listing provides protection from insider trading laws, but not from criminal liability. In private transactions, in particular, there is a risk of criminal liability for breach of fiduciary duty under Art. 158 of the Swiss Criminal Code.

03 Front-running and back-running are not trivial offenses. Anyone who exploits an information advantage in the context of private investments risks criminal consequences, even without malicious intent.

04 Clear internal processes and early legal advice are the most effective protection against criminal liability and reputational damage.

Michael Mráz
Partner
m.mraz@wengervieli.ch
+41 58 958 53 18

Loris Baumgartner
Senior Associate
l.baumgartner@wengervieli.ch
+41 58 958 53 44

Wenger Vieli is your reliable partner in legal and tax matters. Not only do we pride ourselves on bringing outstanding professional skills, experience, and a sense of responsibility to the table, but we are also highly inquisitive! Where others see obstacles, we see opportunities, find solutions, and open up new horizons. We do this with pleasure. In Switzerland, Europe, and the rest of the world.

© Wenger Vieli Ltd., 2026

Disclaimer: The information contained in this publication is intended for general information purposes only and does not constitute legal or tax advice. This content is not meant to replace individual advice from competent professionals in a specific case.