# THE RISING RISK OF BUSINESS IDENTITY THEFT:

# WHY FORMAL ENTITY DISSOLUTION AND WITHDRAWAL IS A CRITICALLY IMPORTANT SAFEGUARD

**"Identity thieves scour government sites searching for corporations listed as delinquent or suspended, with the implication being the owners or managers are not paying attention."**

Thanks in part to the massive migration of data online, identity theft has become more prevalent in recent years. The Consumer Sentinel Network Databook 2020, published by the Federal Trade Commission (FTC), illustrates the scope of the problem. According to the report, the FTC received 2.2 million reports of fraud from consumers that resulted in a total loss of $3.3 billion dollars.

While the focus of identity theft has generally been on the breach of personal data, business identity theft is also a significant phenomenon. Business identity theft (sometimes referred to as commercial or corporate identity theft), has grown increasingly popular with criminals as they seek to exploit security holes associated with business practices and governmental data collection.

Criminals have been exploiting what has long been a common (if ill-advised) practice for some companies: Failing to formally dissolve in a home state—or withdraw registration in qualified foreign states—after becoming inactive.

When a corporation fails to dissolve or withdraw it remains on the public record, meaning it may still be required to satisfy a variety of obligations, including paying franchise and state taxes, and filing annual reports. Failure to fulfill these tasks will lead to a corporation being suspended, declared delinquent, or otherwise adjudged to be not in good standing. This chain of events will ultimately lead to administrative dissolution within the home state and revocation of the certificate of authority to do business in other (so-called "foreign") states.

More concerning, allowing an administrative dissolution or revocation exposes a firm to business identity theft. This is why it is recommended for law firms to strongly encourage their clients to take the appropriate steps to formally dissolve or withdraw their businesses. Doing so is an essential step in mitigating the possibility of business identity theft.

## WHY BUSINESS IDENTITY THIEVES TARGET CORPORATIONS AND LLCS

Identity theft, like many illegal acts, is often a crime of opportunity. Thieves probe for vulnerabilities and then exploit them. In terms of corporations and LLCs, identity theft can be successfully undertaken using information that is publicly available on most Secretary of State websites. In this way, criminals exploit standard "good faith" rules of operation.

Identity thieves scour government sites searching for corporations listed as delinquent or suspended, with the implication being the owners or managers are not paying attention.

*continued on page 2*

Criminals also harvest other useful data, such as EIN numbers, that are available online or via a simple information request. Since there is no mechanism governing who can request such information, identity thieves can collect this data at will.

Once this information is possessed, it's relatively simple for identity thieves to take the steps to place a corporation or LLC back into good standing, or reinstate it if it has been administratively dissolved or revoked, without the owner's knowledge. Often this is as simple as creating a new mailing address, where thieves can receive a new certificate of good standing. This maneuver, which is hard to detect, is often just as difficult to reverse—with devastating consequences for the business owners.

## THE FINANCIAL CONSEQUENCES OF BUSINESS IDENTITY THEFT

Once a criminal has reinstated a corporation or LLC, or placed it back into good standing, the criminal may now appear to have the authority to act on behalf of the victimized company. This means that new loans or lines of credit may be taken out and new contracts signed.

Making things worse, business identity theft can threaten the personal liability protection offered by the corporate or LLC structure. This could potentially make victims liable for any debts incurred by the business identity thieves.

Fraudulent tax returns are another key area of concern. In 2020, the Internal Revenue Service conducted close to 1,600 investigations that uncovered $2.3 billion in tax fraud.

### *Additional risks and consequences*

Along with financial liabilities, businesses that are not formally dissolved or withdrawn also risk sanctions from states. Failure to satisfy corporate or LLC filing requirements, taxes etc. may result in additional fines or penalties being assessed.

Potential liability is another important concern. Corporate officers or directors who are judged to be responsible for failing to formally dissolve—and subsequently failing to monitor and prevent violations—may be targeted in a derivative suit.

**"Recent reports have definitively shown that business identity theft is both a serious problem and a rising risk for corporations and LLCs."**

Additionally, some states have specific laws that extend such liability to employees or officers who are responsible for a firm's tax returns or payments, and who willfully or knowingly fail to make payments.

## CONCLUSION

Recent reports have definitively shown that business identity theft is both a serious problem and a rising risk for corporations and LLCs. Law firms have a key role to play in combating this trend.

Law firms should advise their clients to take the relevant affirmative actions in order to voluntarily and safely dissolve or withdraw their entity. Doing so will help ensure that these clients do not face the elevated risk of business identity theft—and end up paying the high financial price of non-compliance.

Learn more about how CT can help with properly dissolving your client's business including tasks such as filing dissolution, termination, and withdrawal documents and final annual reports, obtaining tax clearances, and canceling business licenses and assumed names.