The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 12, No. 9 September 2004

Service Mark Counterfeiting And Worse: U.S. Companies Resort To Self-Help In Canada When Cross-Border Law Enforcement Falls Short

Bruce A. McDonald

WILEY REIN & FIELDING LLP

One of the most damaging infringements that a well known company can experience occurs when infringers counterfeit the name and address of the company in the course of, or as a means of engaging in, consumer fraud or other criminal activity. In the financial services industry, the names and addresses of many well known companies are counterfeited in the course of telemarketing and wire fraud. The challenges facing such companies in the case of anonymous counterfeiting can be particularly daunting when the counterfeiting occurs in a foreign country such as Canada and the damage is suffered by consumers in the U.S.

In the past five years, cross-border telemarketing fraud by Canadian imposters against U.S. consumers has become a booming industry. Heading the list of fraudulent schemes is the so-called "advance fee loan" scam. Of some 5,000 complaints received annually by law enforcement authorities in Ontario from U.S. consumers, 75% involve "advance fee loans."

In the "advance fee loan" scam, unidentified imposters use stolen credit cards and fictitious addresses to obtain toll-free numbers and cell phones in Canada which they use to place advertisements in the classified sections of U.S. newspapers such as the following:

> **NEED CASH?** Financial help available for 1st & 2nd mortgages, student, business & personal loans up to $500,000. Fast approval. Low daily rates. Call 1-800-123-4567.

Bruce A. McDonald

U.S. consumers who respond to such advertisements reach individuals who hold themselves out as representatives of well known U.S. financial services firms. The imposters interview the U.S. consumers, take their personal and financial information, and then fax them packages of counterfeit "loan documents" bearing the financial service company's name and service mark.

In follow-up telephone calls, a perpetrator informs the consumer that the latter has been approved for credit and that the desired loan will be disbursed directly into the consumer's bank account upon the advance wire payment of an "insurance" fee. When the U.S. consumer wires the "advance fee," the imposters or their accomplices appear at a wire services location and disappear with the money. The U.S. consumer never sees his money again, much less the promised loan.

According to the Toronto Police Fraud Squad Telemarketing Section, 15,953 incidents of advance fee loan fraud were reported to Canadian law enforcement between 1996 and 1992, accounting for $10,716,476.41 in losses to U.S. consumers.[1] In turn, 3,783 complaints were received by the Federal Trade Commission in 2003 from U.S. consumers involving cross-border advance fee loan scams originating in Canada.[2]

All of this is a nightmare for the U.S. company whose name and address were counterfeited by the perpetrators. Defrauded consumers flood the service mark owner with telephone calls, believing they have been swindled by the service mark owner.

Identification of suspects and the enlistment of assistance from law enforcement authorities are the principal challenges faced by service mark owners in these instances. Identification of suspects is exceptionally challenging due to sophisticated measures undertaken by the perpetrators to evade detection. Nonetheless, a private investigator retained by the U.S. service mark owner can discover a surprising amount of information about the telephone numbers used by the perpetrators.

In fact, U.S. private investigators may have an advantage over their Canadian counterparts, whose ability to obtain telephone records is relatively constrained by stricter adherence to privacy standards in that country. The U.S. private investigator may even have an advantage over the Canadian police, whose ability to tap phones and obtain private records requires a court order and is otherwise limited by the Canadian equivalent of probable cause.

In general, technological advances in the ability to discover almost anything about almost anybody, almost anywhere, almost immediately, may lead to a disturbing dis-

Bruce A. McDonald is a Partner in Wiley Rein & Fielding's Intellectual Property, International Trade and Internet & E-Commerce Practices. He can be reached at 202.719.7110.

Please email the author at bamcdonald@wrf.com. with questions about this article.

crepancy between information that can be *lawfully obtained* and information that is *actually possessed.* To what extent the service mark owner is responsible for his U.S. investigator's compliance with Canadian privacy laws, bearing in mind that the subject of his investigation is a criminal ring engaged in the counterfeiting of his trade name and service mark, and how to handle sensitive information that comes into the service mark owner's possession through sources and methods of third parties contracted by his investigator, which sources and methods may be difficult or impossible to discern, are exceptionally sensitive and difficult issues. For present purposes, it suffices to state that a private investigation *can* lead to the discovery of information that either identifies the responsible individuals, or *would be* sufficient to establish the identity of the responsible individuals, *provided that* Canadian police were available to kick down doors or otherwise complete the steps that cannot be undertaken without color of authority.

The heart of the problem is that the enlistment of assistance from U.S. and Canadian law enforcement authorities may be even more challenging than identification of the suspects, due to the vagaries of cross jurisdictional issues. While consumers in the U.S. are suffering the brunt of the damage, effective recourse requires aggressive investigation and prosecution by Canadian police. In a law enforcement milieu of limited resources, competing priorities, and multiple jurisdictional questions, the problem has a tendency to fester.

Failing successful efforts to identify and apprehend the responsible individuals, or to obtain assistance from U.S. and Canadian law enforcement authorities in apprehending and prosecuting such persons, service mark owners may be required to take action that is essentially *in rem*, for example, to terminate a toll-free telephone number used by the perpetrators, or to seize a bank account where proceeds from the illicit activity are deposited.

Canadian authorities have made a number of arrests. However, for the most part, the Canadian perpetrators have evaded apprehension by using sophisticated arrays of telecommunications hardware in warehouses and low-income housing projects outside of Toronto to "bounce" calls and messages from one physical location to another.

The initial recourse of U.S. financial services firms, when the perpetrators cannot be identified, is to report the counterfeit use of their names and addresses in criminal complaints filed with Canadian and U.S. law enforcement authorities. However, both U.S. and Canadian law enforcement authorities are overwhelmed by work loads with issues such as terrorism and national security demanding top attention. Consequently, the service mark owner's problems with telemarketing and wire fraud is likely to find itself on the "back burner."

Service mark owners in these circumstances thus have to investigate the possibility of "self help." The service mark owner may attempt to set up a "sting," using a private detective posing as a consumer seeking a loan, in an effort to identify the perpetrator when the latter appears at the wire services location designated in the perpetrators' payment instructions.

However, a successful "sting" poses daunting obstacles. First, there is no guarantee that the perpetrator will appear at the designated location, since, with the use of "transit numbers," claimants can collect wire transfers at any location.

Second, even if the perpetrator appears at the designated location, a "sting" requires the cooperation of the wire services company. The clerk at the wire services company must somehow notify the private detective when the perpetrator appears to claim his payment. The wire services company may be reluctant to participate, even passively, in a third party's efforts at private law enforcement, particularly if it perceives any element of risk to its employees.

Finally, the question arises, what does the private detective do if he is able to identify the perpetrator in a successful "sting"? The image comes to mind of the swift-footed canine who "catches" the car he his chasing. Service of a lawsuit on such a "John Doe" defendant may be an insufficient (if not comically ineffective) measure, in which case the private detective will need to follow the perpetrator in a continued effort to identify the responsible individuals.

Whether service mark counterfeiting is committed in the course of "advance fee loan" fraud or any other form of criminal activity, the success of a private investigation is measured by its ability to identify the names (*i.e.*, the real names, not the aliases) and addresses of the perpetrators. At that juncture, the service mark owner has a choice of pursuing civil remedies or approaching law enforcement authorities with a "complete package" that enables (if not effectively compels) the authorities to apprehend the responsible individuals.

The "holy grail" of any private investigation is to identify a bank account (in the U.S. or elsewhere) where proceeds from the illicit activity are deposited. If such a bank account is identified, a service mark counterfeiting action can be filed against "John Doe" defendants in the jurisdiction where the involved bank is located. A subpoena can then be served on the bank, accompanied by an *ex parte* order freezing the account.

Acting on mutual concerns over the use of counterfeit names and addresses by advance fee loan perpetrators, a group of financial services companies converged as joint plaintiffs in a "John Doe" action filed in 2003 before the Ontario Superior Court of Justice.[3] The plaintiffs in that action sought an order that would require Canadian telephone companies to shut down any toll-free telephone number that could be shown to have been used for an advance fee loan fraud. This Canadian court action resulted in an unopposed order in which a number of Canadian telecommunication service providers agreed to accept a sworn statement from those plaintiffs whose names and addresses had been counterfeited, for the purpose of shutting down any telephone account that fraudulently referred or related to one or more of those service mark owners.

In all other cases, *i.e.*, those involving different service mark owners or different Canadian telephone companies, the service mark owner may go directly to the Ontario Superior Court of Justice, institute a "John Doe" action, and obtain a court order requiring the Canadian telephone company to cancel the fraudulent toll-free number.

Of the remedies described above, no single one is perfect. A court order shutting down a single toll-free number poses difficulties similar to those confronting Hercules in his struggle against the multi-headed Hydra. No sooner does the Canadian telephone company cancel the toll-free number in response to the service mark owner's court action, than the fraudulent advertisement reappears in U.S. newspapers with a new toll-free number.

Efforts to identify and apprehend persons responsible for the counterfeiting of U.S. financial services companies' names and service marks, whether in the course of "advance fee loan" fraud or other telemarketing fraud, are underway in multiple jurisdictions. Fundamentally, the problem is one of criminal law enforcement, and ideally, the problem would be aggressively addressed by the responsible authorities. Effectively, however, service mark owners must consider the various measures discussed above.

---

[1] *Federal Trade Commission*, Cross-Border Fraud Trends, January – December 2003 *(March 14, 2004), at 9.*

[2] Id.

[3] Sun Life Assurance Co. of Canada et al. v. John Doe, *Court File No. 03-CV-253452CMI (Ontario Superior Court of Justice).*