LexisNexis®
RISK SOLUTIONS

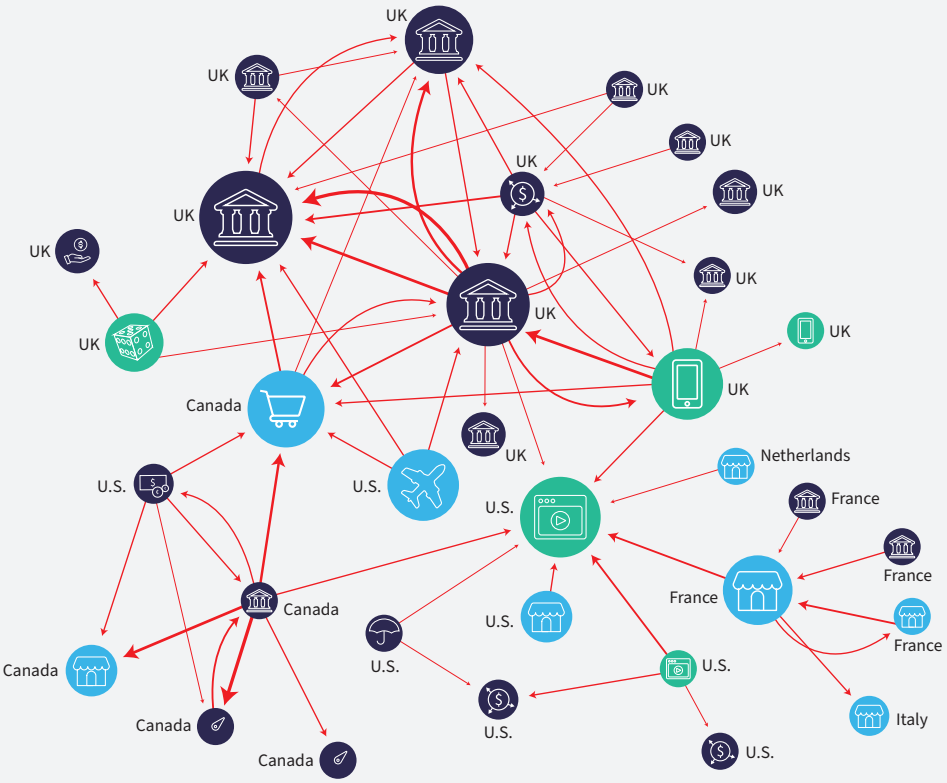
ALONG CAME A FRAUDSTER

Understanding the Spider's Web of Networked Fraud

As we move into springtime, many of us will embark on Spring cleaning; clearing the dust and clutter of the winter months out of our homes, readying for the warmth of spring and summer. Whist helping a family member in said spring cleaning, I quickly came to realize the main adversary in such a task - cobwebs – of which there were plenty. While wrestling with the webs, hoping in vain to avoid their makers, I came to realize that webs are simply a series of connections, a pattern in which to lure and trap prey. Failing to separate work from spring cleaning, I thought about the other webs which are weaved, thinking to the latest LexisNexis® Cybercrime Report, and came to the conclusion that webs are not the sole domain of spiders.

Indeed, fraudsters are becoming adept at creating their own interconnected networks, operating across organizations, industries and country borders. Just like a spiderweb, these networks are intricate, strong and rapidly built, luring consumers and tricking organizations. You many think I am being hyperbolic, but just look at the global fraud network centred around UK banks which was uncovered in the cybercrime report.

This global network, the largest individual network analysed in the report, was uncovered by the LexisNexis® Digital Identity Network®, and bore all the hallmarks of a fraud network, including the extended spider's web of mule activity that is fed by this fraud. This network encompassed several UK banks and lenders, financial services institutions in the U.S., Canada and France, as well as retailers and media companies that span all regions. This huge mule network was linked with thousands of devices and transactions, all engineered to maximize reach across unsuspecting consumers and organizations.

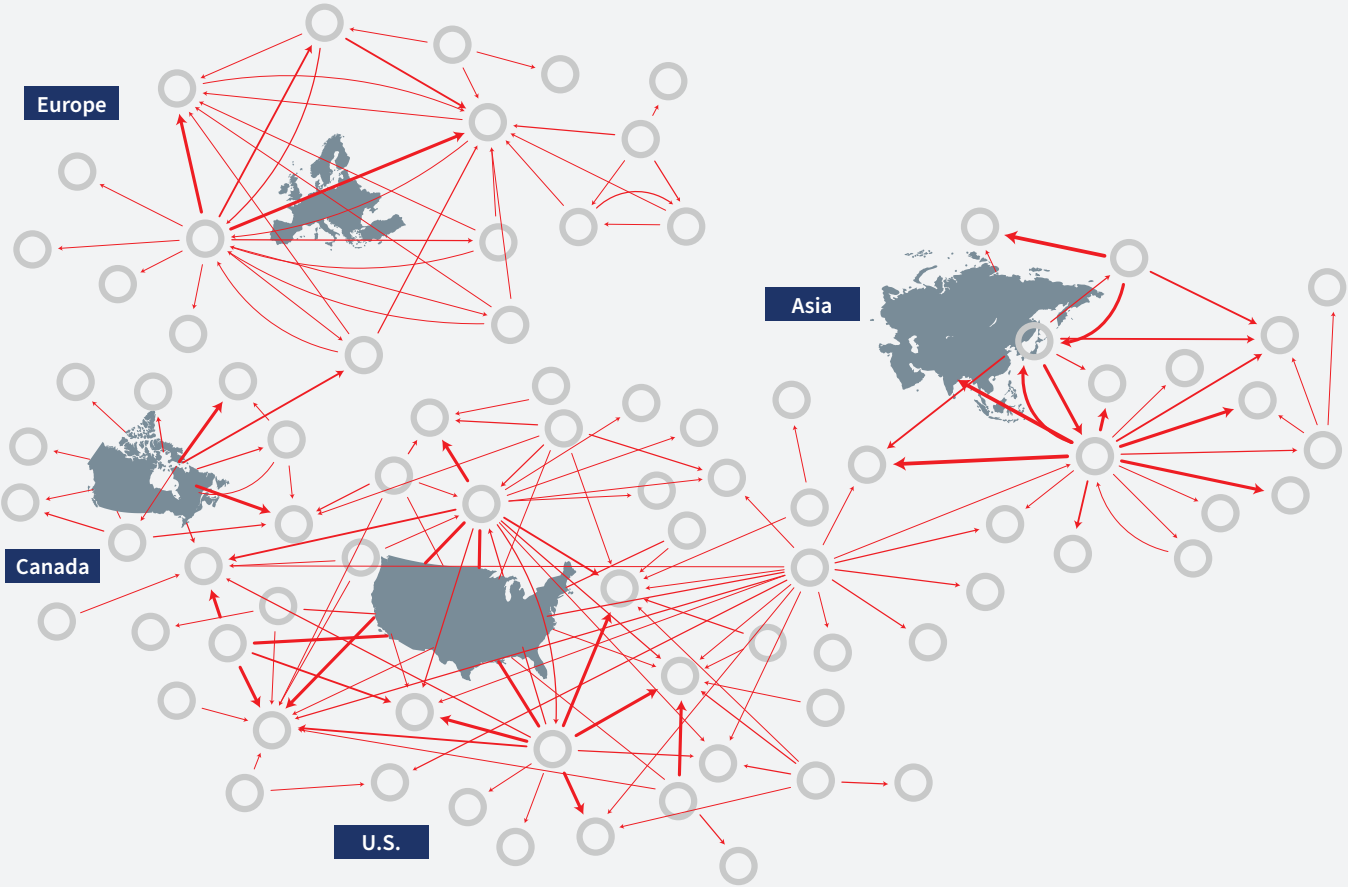


A larger circle denotes a larger organization by transaction volume. A thicker line denotes a higher volume of fraud. Less than 10 device overlaps between companies have been removed.

This size and scope of networked cybercrime really hits home in the visualization below taken from the cybercrime report. It shows a global fraud network made up of several smaller interconnected networks.

Each circle represents one organization, with each arrow illustrating fraud originating from one organization and crossing over to another, separate, organization. A thicker line denotes a higher volume of fraud – akin to how the strength of a spiderweb is dependent not only on the strength of the spun silk, but also on the design of the web.

What this shows is that these webs of fraud, or hyperconnected fraud networks, not only exist locally, but also regionally and globally. The price of such networks can be innumerable. The monetary cost alone can be huge, in addition to brand and reputational losses – the aforementioned fraud network centred around UK banks had $12.5M exposed to fraud in just one month.



LexisNexis® RISK SOLUTIONS

So, the question is, how do we fight back against these networks? How do we protect our customers and better detect cybercrime from increasingly sophisticated fraudsters?

If we were still only talking about cobwebs, I may advise you to strategically place conkers around the house (an old wives' tale which I've been led to believe), however, the webs of deceit spun by fraudsters will need much more robust defenses.

In order to fight highly networked, complex and ever-evolving cybercrime, businesses must no longer rely on mitigating individual attacks using point solutions. Instead businesses must almost mirror the fraud typologies they need to defend against: networked, layered, inter-connected and operating without borders.

Businesses must adapt to the evolving cybercrime landscape, embracing and deploying the next generation of networked fraud detection capabilities, such as;

The development of payment network profiling, linkage and network visualizations.

Advanced behavioral biometrics capabilities that expose inherent user behaviors without compromising privacy, or introducing unnecessary friction.

Cross-organizational / cross-industry data sharing via dedicated consortia.

Network identification of first, second and third-party fraud risks.

Next-generation bot data management and risk intelligence signals.

It is in the layering of these market-leading innovations that a true network of fraud defenses can be built to tackle the most complex and constantly growing global fraud networks.

Although Spring cleaning rids our houses of spiderwebs, we know that they will return and that we will have to repeat the spring cleaning every year. The web may be spun by a different spider, in a different place, but the web will still be engineered to trap prey. Similarly, the webs spun by fraudsters, weaving across organizations, industries and regions, are in a constant state of flux.

To avoid being caught in the fraudsters' web, businesses must analyse individual fraud attacks, implement effective mitigation strategies, and share information relating to known fraudsters across businesses facing the same challenges. Conkers, unfortunately, will just not do.

LexisNexis® RISK SOLUTIONS

For more information,
visit risk.lexisnexis.com/FIM-EN