FROM KINETIC TO SYNTHETIC

An extract from Perspective:
The fraud and identity issue
Essential insights into the issues facing your industry today

EQUIFAX®

Keith Manthey, CTO Analytics, Emerging Technologies Division at EMC², talks to Perspective about the risks presented by synthetic identity creation and how businesses can best protect themselves from cyber fraud.

2016 is upon us and technology continues to evolve and drive disruption. By now, most of you have probably viewed the meme being shared online that lists the biggest online taxi company as having no cars, the biggest accommodation company as having no property, etc. The identity and fraud space has not been unaffected by this trend either.

Several decades ago, identity and fraud were presenting business with a challenge, but the challenge was very kinetic. A fraudster usually committed the fraud in person and often used forged documents to commit the crime: fraud was therefore a very physical or kinetic transaction.

Fast-forward to today and kinetic fraud has greatly reduced in scope and impact; in its place, cyber fraud (committed via many different avenues) is burgeoning. Taking into account a number of recent cyber breaches, identity information and compromised payment methods like credit cards are readily available on the dark portions of the web. These identity elements sell for extremely low monetary values these days but it's the volume of this data that will ultimately be financially rewarding to the fraudsters.

Danger on the cards?

While 'Chip and PIN' technologies with Europay, Mastercard and Visa (collectively known as EMV) are in place to help prevent compromised payment methods, those individuals who will typically visit the dark places of the web will have already subverted some of these 'Chip and PIN' elements. 'Chip and PIN' cards or EMVs are implanted with a computer chip that provides an additional layer of security to payment cards than was previously available on the magnetic stripes on the back of non-EMV cards.

EMVs are far more secure than the non-EMV chips when it comes to protecting against the 'cloning' of the card. In order for an EMV card to be compromised, hackers must be able to interrupt an active payment transaction. This isn't an easy proposition.

For businesses in 2016, risk mitigation is a natural part of their operations. The shipment of products to individuals paying with compromised payment methods is a risk that will only become harder to manage. The creation of new payment accounts using identity elements bought on the dark web (like name and address details along with phone numbers) presents another set of risks for financial institutions. Prudence and diligence are two things that are critical in today's environment.

Changes in challenges

For retailers, creating a medium to ensure that buyers, and their means of payment, are legitimate is becoming increasingly difficult. Mobile payments are also increasing in frequency and volume, which also add to the challenge. It's no longer easy to track a customer across all their devices as cookies can be turned off and locations aren't always available.

Retailers could protect themselves more effectively just by adding a few extra minutes to sales transactions: firstly, requiring a customer to create a new account instead of allowing a 'guest check out'; secondly, using an address verification system associated with payment cards if the shipping address is different from the billing address of the card; and thirdly, using a robust fraud scoring system (such as amount of sale, proxy detection, geo and IP filtering) for each transaction.

The rise in synthetic identities

Synthetic identities (or identities created through an amalgam approach) created from the dark web will continue to be a tool favoured by cyber criminals. A good example of a synthetic identity would be a real name, a known address (like a closed business, a vacant home or a post office box) from which a fraudster could operate and a phone number where a fraudster answers the phone. A good synthetic identity is often easily confused with the real person, so the address used will often be close to that of the known individual whose identity fraudsters are attempting to clone.

There are a number of companies that monitor dark web identities that are being traded and who ply their services to legitimate industries that attempt to protect their clients, like Credit Reference Agencies. It would be interesting for financial services companies to use this kind of dark web-traded information to prevent new synthetic identities from being created.

In addition to tracking the dark web, sound business practices to ensure only legitimate identities are being created are the key to curbing risk losses. Businesses also need to make use of existing tools, like credit reports and other data sources, in the battle to limit the number of synthetic identities that slip through the net. Synthetic identity fraud can only be mitigated if companies are able to combine the use of established methodologies with newer analytical techniques.

CLICK HERE FOR MORE ARTICLES