GLOW TOUCH

Every 22 seconds *That's how often identity theft occurs*

The number of fraud and identity theft cases has almost tripled over the last ten years, growing into a multi-billion dollar per year criminal enterprise that shows no signs of slowing down. The market for protection services is growing, too, to keep pace with – if not get ahead of – an increasingly sophisticated network of thieves who sell each other tools and data.

Their work has victimized almost one-third of Americans have been victimized. While traditional schemes such as phishing, its telephonic cousin – vishing, and credit card fraud remain proven methods, new approaches are being developed to take advantage of technological innovation and consumer laxity. Ransomware is a huge concern among organizations, primarily because it works. When nearly three-quarters of companies are impacted by at least a portion of the ransom demand, that will only incentivize more of the same.

Did you know

- Every data breach costs nearly **$4 million**
- More than **one million** children are victimized every year
- The most common victims are **30-39**
- Total losses to cybercrime are more than **$10 billion**
- Trying to keep pace

At the individual level, synthetic fraud has entered the scene, coupling factual information like Social Security numbers with false names. These fake accounts can be used to make large, immediate purchases or to build a high credit limit that is then maxed out with the balance left unpaid. In the worst case, a crime ring spanned multiple states and racked up $200 million in losses to merchants and individuals. More synthetic fraud is among the trends expected to increase.

What's coming

A lot of personally identifiable information (PII) stolen in early 2020 is expected to surface in the next few years. Scammers thrive in periods of uncertainty, offering fake assistance that requires people to give out Social Security or bank account numbers and other personal information that is then used fraudulently. Other trends include:

- Account takeover fraud which involves impersonating someone to open an account and using that account to bypass security
- Small and medium-sized businesses will remain vulnerable to fraud due to limited resources and a lack of cybersecurity expertise.
- Social media takeovers, in which **27%** of individuals and **87%** of businesses lost money
- The sword of technology cuts both ways**
    - Impostor scams, particularly those involving deep fake technology
    - The use of machine learning and artificial intelligence will become more widespread in battling fraud by identifying patterns and anomalies in data

This merits a highlight as it points to two things:

1. There is no starting or ending point, just an ongoing cycle of preventive measures, attacks, remediation, new preventive measures, more attacks, and so forth.
2. The same technology that provides us the convenience of working, banking, shopping, and socializing online can also be used against us. This is particularly true among mobile devices and the rise in remote work; people's devices can be hijacked and used as portals for entering corporate networks.

GlowTouch Global Headquarters
9931 Corporate Campus Dr, Suite 1400, Louisville KY 40223
+1 (502) 410-1732 | info@glowtouch.com

All is not lost

A strategic principle with various applications is that the best defense is a good offense. In other words, be proactive rather than reactive. At the organizational level, this includes using artificial intelligence as an early warning system that notices irregular activity and responds accordingly. This capability is invaluable because it focuses on prevention rather than detection. There are other tactics as well:

- Zero-trust access: based on assuming the worst of anyone trying to enter a network, this methodology includes multi-tiered access control, with users required to undergo continuous validation using multiple authentication methods.
- Having the necessary security certifications to set a baseline of standards. Earning certs sends a message of taking risk mitigation seriously. The lack of compliance can also hinder entry into specific markets. This can be as simple as HIPAA compliance for working with healthcare industries and PCI compliance for handling online payments, or it can go deeper regarding information security and protocols for preventing breaches.
- Cyber insurance is a growing market as a hedge against more frequent and more complex attacks. This also couples with certifications since there is no universal standard for doing "enough" to ward off scammers.

For individuals, there are also measures that can be taken:

- Multi-factor authentication, such as a code that augments the user's password.
- Biometric authentication, such as a thumbprint or facial recognition technology, can also eliminate having to remember complicated passwords.
- Password-less technology services that maintain different, hard-to-break passwords for individual accounts so that if one account is compromised, the others are safe
- Frequently checking one's credit reports to spot unusual fluctuations that could mean someone has opened a credit card account in your name

Very few organizations and individuals do nothing. The more significant issue is whether they are doing enough and is what they are doing beneficial?

How we fit in

As a provider of outsourcing services, our clients trust us with their most valuable asset, their customers. That means protecting their customers' data and privacy. We feature the key certifications that mark information security and have others as well. In short, keeping watch over client data is as integral to our service model as providing their customers with world-class support. On a more granular level, these are three examples of our experience within this industry:

- An identity protection services company that provides digital solutions for individuals and organizations alike. Each new data breach brings increased demand for this client's services. When we began, it was to handle the overflow that the internal support team could not manage. Since then, we've not just become a permanent fixture; we have grown the program in size and scope, adding dedicated teams focusing on new member welcomes, existing member retention, and sales.

- When companies are breached and pay settlements to those effective, another requirement is to provide impacted customers with a monitoring service. That's what this client does, and the program has tripled in size since its inception. Our agents deal with transaction alerts on issues such as new loan originations or credit card limits being reached, help desk questions on account management issues, and, most importantly, responding to cases of someone being hacked. The latter can involve calls that last up to 90 minutes, helping the customer contact everyone from financial institutions to government agencies and providing templated letters if necessary.

- This VPN and online privacy service provider had never before outsourced customer support. Today, our team works 24/7 supporting a tech-savvy clientele, meaning our agents must be exceptionally knowledgeable to establish credibility with end users. Along with technical support for customers, we developed a proprietary firewall, which speaks to the unique IT skill level that makes us The Uncommon BPOTM. Many of this client's customer base lives in nations where Internet usage rules are far stricter than those in the US. We help them access a variety of information that might otherwise be unattainable.

The computing-industrial complex is an ever-changing marketplace of innovation, shifts in consumer demand and expectation, and, as the subject matter makes clear, conflict. In an omnichannel world, everything from email to texting to instant messaging to social media is fair game. Each new development translates into a new potential vulnerability to defend for service providers and a new possible weakness to exploit for criminals.